FACULTAD DE INGENIERIA Y CIENCIAS AGROPECUARIAS

DISEÑO E IMPLEMENTACIÓN DE LA RED DE DATOS DE URBANO EXPRESS SOBRE UNA RED MPLS UTILIZANDO EL MÉTODO DE VRF LITE Y MONITOREO MEDIANTE OBSERVIUM.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones

Profesor Guía

Ing. Ricardo Xavier Ubilla Gonzalez

Autor

Cristian Santiago Bustos Sanchez

Año

2016

DECLARACIÓN PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con la estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

_____

Ricardo Xavier Ubilla Gonzalez

Ingeniero en Electrónica y Telecomunicaciones
CI. 091756564-0

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Cristian Santiago Bustos Sanchez

CI. 150086311-1

AGRADECIMIENTO

Agradezco a mi madre y hermanas, que han sido las personas que me han dado fortaleza y apoyado de manera incondicional en todo momento.

Al Ing. Edison Pérez e Ing. Ricardo Ubilla, quienes me han orientado en todo momento en la realización de este proyecto que es un escalón importante para cumplir mis objetivos y metas.

DEDICATORIA

A mi madre y hermanos porque creyeron en mí, me han dado ejemplos de superación y entrega para llegar a cumplir mis metas sean académicas o personales, siempre estuvieron impulsándome en los momentos que más necesitaba de ellos.

También, dedico a Diana ya que ha sido la persona que ha estado incondicionalmente apoyándome.

RESUMEN

El proveedor de servicios de internet (ISP) Puntonet, presta los servicios de datos y acceso a Internet a la empresa Urbano Express (véase en anexo 1) a nivel nacional, con el fin de mejorar los servicios prestados y garantizar un servicio óptimo, se migró de una red Metro Ethernet a una red multiprocol label switching MPLS, este objetivo se logró con una serie procesos que a continuación se menciona.

Se realizaro un análisis de la red que se encontraba funcionamiento en Metro Ethernet, para lo cual se investigó el direccionamiento, enrutamiento, topología, ancho de banda, servicios y los equipos que estaban operando en cada uno de los enlaces a nivel nacional, posteriormente se analizó toda la información y se propuso un diseño óptimo de la red con la nueva tecnología MPLS.

El diseño de la nueva red se implementó en cada uno de los enlaces dentro de un cronograma establecido, el cual empezó con la matriz de Urbano Express, donde se instaló un router en paralelo, para no afectar el funcionamiento de la red que en ese momento se encontrataba operando, este router se encuentra en la nueva red MPLS y tiene configurado VRF lite, BGP, route-map, prefix-list y redundancia a nivel de la última milla, brindando los servicios de datos y acceso a Internet simultáneamente, posteriormente se migraró cada sucursal.

Cada uno de estos enlaces que se están en la nueva red MPLS, fuerón ingresados al software de monitoreo Observium, permitiendo de esta manera tener un monitoreo de consumo de ancho de banda y disponibilidad del enlace.

Una vez que todos los enlaces se encuentran en la nueva tecnología, se procedió a verificar la convergencia de toda la red y el funcionamiento correcto de la misma.

ABSTRACT

The internet service provider ISP Puntonet provides data services and internet services to the Urban Express business nationwide, in order to improve services and ensure optimal service, was migrated from a Metro Ethernet network to a multiprocol MPLS label switching network, this was achieved through a series processes mentioned below.

An analysis of the network operation was in Metro Ethernet, for which addressing, routing, topology, bandwidth, services and equipment that were operating in each of the links at the national level was investigated, them analyzed all information and optimal network design with the new MPLS technology was proposed.

The design of the new network was implemented in each of the links within an established schedule, which began with matrix, where a router was installed in parallel to not affect the operation of the network at the time is operation, this router is in the new network MPLS and has set VRF lite, BGP, route-map, prefix-list level redundancy and the last mile, providing data services and Internet simultaneously, then each branch is migrated.

Each of these links, which are in the new MPLS network will be entered observium monitoring software thus allowing to have a consumption monitoring bandwidth and link availability.

Once all the links are in the new technology, we proceeded to verify the convergence of the entire network and proper functioning of the same.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCIÓN

Tema: Diseño e implementación de la red de datos de Urbano Express sobre una red MPLS utilizando el método VRF LITE y monitoreo Observium.

El proyecto plantea una topología de red que no utiliza subredes en la interfaz túnel creada en cada router local y remoto del cliente, tampoco se utiliza subredes con IP públicas, debido a que se emplean para cada enlace subredes de 4 IP privadas y una sola virtual routing and forwarding VRF que permite conectividad de la red, en esta topología el router CE de cada sucursal a nivel nacional se configura directamente en los routers de backbone (PE) al que corresponda y mediante la red de transporte MPLS de Puntonet S.A. a nivel nacional, por el protocolo BGP se establecerá las comunicaciones entre sucursales y matriz.

En los enlaces de las sucursales y matriz se implementará la configuración de protocolo de enrutamiento Costos directos técnicos dinámico en el CE y PE con un sistema autónomo de EIGRP similar para todos las sucursales, los enlaces se cuentan con servicios de internet y datos, utilizará la misma última milla principal como backup en un solo router Cisco o Mikrotik, en el cuál, mediante el método de VRF LITE se efectuará routers virtuales para cada servicio y será entregado una interfaz independiente.

La implementación se realizará con IPv4 debido que el ISP Puntonet.SA, todavía no tienen difundido e implementado en la red de backbone con IPv6; sin embargo, como aporte adicional al desarrollo del proyecto también se realizará el diseño en IPv6.

Antes de iniciar las migraciones de las sucursales se instalará un router en paralelo en matriz, para migrar según el cronograma, cada sucursal podrá trabajar normalmente por la antigua conexión hasta que se proceda a migrar. En las sucursales se procederá a respaldar las configuraciones actuales de los

equipos, antes de proceder a realizar las nuevas configuraciones, cada sucursal tendrá una ventana de mantenimiento de 30 minutos, se procederá a migrar a la nueva tecnología MPLS, se efectuará las pruebas de ancho de banda, conectividad con matriz y resto de sucursales.

Todos los enlaces que se migrará a MPLS se ingresaran en observium para un monitoreo respectivo y un soporte eficiente.

Objetivo General

Diseñar e implementar la red de Datos MPLS para la empresa Urbano Express, que represente una solución versátil con múltiples ventajas a nivel nacional.

Objetivos específicos

- Realizar un estudio de la situación actual de la red de comunicaciones y transporte entre matriz y sus diferentes sucursales.
- Utilizar un método eficaz para proporcionar los servicios de datos e internet.
- Integrar los enlaces de la red MPLS en el servidor web para un monitoreo eficiente y proactivo.
- Emplear un protocolo de enrutamiento dinámico para enlaces de backup utilizando diversas tecnologías de accesos.
- Difundir las subredes LANs de cada sucursal en la red MPLS mediante un protocolo de enrutamiento.
- Mejorar el rendimiento de la red minimizando costos de implementación.

1. Capítulo I. Marco Teórico

1.1 Redes de Acceso

La red de acceso es esencial para las comunicaciones de las redes, porque es el medio que permite llegar al usuario o cliente final desde el punto más cercano de la red de transporte o backbone del proveedor. Trabaja a nivel de la capa física y enlace en el modelo de interconexión de sistemas abiertos OSI (véase anexos 1), y claramente está clasificada en dos grupos guiados y no guiados.

Los medios guiados generalmente utilizan medios físicos como el cable utp (véase anexo 1), coaxial, fibra óptica, etc. estos medios de transmisión permiten manejar un mayor ancho de banda, pero su instalación es más compleja que un medio no guiado como radio enlace, enlace satelital, etc., los cuales al utilizar el espacio aéreo como medio de propagación, permiten una instalación menos compleja.

1.1.1 Fibra Óptica

La fibra óptica es uno de los medios de transmisión más utilizado en las redes de telecomunicaciones, por sus características como: gran ancho de banda, alta seguridad, larga duración, inmunidad a interferencias electromagnéticas, baja atenuación y bajo costo con referencia a otros medios de transmisión.

El cable de fibra óptica, está formado por un núcleo con hilo de fibra de vidrio o silicio, que permite guiar el haz de luz a lo largo de la fibra, esto gracias a su índice de refracción elevado, su dimensión es alrededor de 0.1 mm. El revestimiento rodea al núcleo protegiéndolo de fuerzas externas, también cumple la función de cambiar la dirección del haz de luz, debido a que tiene un menor índice de refracción, garantizando que la misma se transporte a nivel del núcleo. La chaqueta protege a la fibra de las diferentes condiciones ambientales, además de interferencias de fibras adyacentes.

Dependiendo de la forma de propagación del haz de luz, la transmisión en fibra óptica se clasifica en: monomodo y multimodo. Las fibras monomodo utilizan como fuente de transmisión un láser, permitiendo anchos de banda iguales a

50 Ghz, velocidad de 622 Mbps y hasta 100 km de distancia. Las fibras multimodo que tienen menor costo, velocidades desde 10 Mbps hasta 155 Mbps y distancias de 2.4 Km (Itlalaguna, s.f. pp. 9 - 14).

1.1.2 Radio Enlace

Radio enlace es la interconexión entre terminales, los cuales pueden ser fijos o móviles mediantes ondas electromagnéticas en frecuencias desde 800 Mhz hasta 426 Ghz, esta comunicación es de tipo dúplex con 2 portadoras moduladas, una para la transmisión y la otra para la recepción.

Varios aspectos se deben considerar en la configuración de un radio enlace como son: la frecuencia de operación, la potencia de transmisión y el más importante el ancho de banda necesario. La disponibilidad de un radio enlace depende principalmente del clima y la distancia entre los terminales.

El radio enlace punto – punto, fue diseñado para la comunicación entre dos nodos específicos, el uno operando en modo de acceso y el otro en modo transmisor, las dos antenas deben tener línea de vista directa, la frecuencia de operación es de 2.4 Ghz y 5.8 Ghz (radiocomunicaciones, s.f.).

El radio enlace punto – multipunto, está conformado por una antena transmisora y por varias antenas receptoras, cada una internamente utilizan MIMO (véase anexo 1) 2x2, es decir, dos trasmisores y dos receptores, las frecuencias de operación son de 2.4 Ghz y 5.8 Ghz cumpliendo el estándar 802.11X.

1.1.3 ADSL

La Línea de abonado digital asimétrico (ADSL), utiliza la línea de cobre (telefónica) como medio de transmisión, al ser asimétrica el ancho de banda de bajada es diferente al de subida, por ejemplo 1024/512 Kbps.

Para este medio de acceso, los parámetros más importantes a considerar son: la distancia máxima de 3 Km desde la central telefónica hasta el módem ADSL, la atenuación máxima de 48 dB, la señal a ruido mínima de 15 dB (véase en anexo 1) y la velocidad que se encuentre dentro del rango de 1.5 Mbps a 8

Mbps. Generalmente se usa con el protocolo ATM (protocolo de transporte que emplea un canal virtual PVC, con un identificar de paquetes virtuales VPI y un identificador de circuitos virtuales VCI), (datateca, s.f, pp. 9 - 11)

1.1.4 VSAT

El Terminal de apertura muy pequeño (VSAT), soporta servicios como datos, video y voz, empleando un satélite que transmite y recepta las señales desde las estaciones terminales hacia un concentrador HUB (véase en anexo 1) y viceversa, este tipo de sistemas son empleados principalmente en lugares donde la cobertura es muy compleja para otro tipo de tecnología como fibra óptica, radio enlace, etc.

Las velocidades de trabajo en los enlaces VSAT son pequeñas por ejemplo 1024 kbps, esto debido a las bandas de frecuencia en las que opera: C, K, Ku, etc. También, determinados servicios o aplicaciones se ven afectados por el retardo de 600 milisegundos característicos de este tipo de enlaces (vsat, s.f, pp. 1).

Algunas ventajas de los VSAT son: cobertura global, fácil y rápida instalación, alta disponibilidad de la red y un costo bajo.

Todas las tecnologías anteriores mencionadas serán aplicadas en la nueva red MPLS.

1.2 MPLS

Multi protocol lebel switching (MPLS) inicia en los años 90, avanzando en el mercado de manera exponencial y adoptada por diversos proveedores a nivel mundial para sus redes de backbone, debido a la necesidad de incrementar la capacidad de sus enlaces, luego de 7 años de su creación se realizaron técnicas de conmutación de diferentes capas o también llamadas multinivel, logrando el estándar actual. MPLS está realizado por dos mecanismos esenciales como son: separación entre las funciones de control (routing) y de envío (forwarding), también se empleó las etiquetas para identificar los circuitos virtuales a lo largo de la red y así poder aplicar calidad de servicio (cisco, s.f, p. 11-20).

MPLS, es una red de nueva generación, debido a que soporta multiservicios, en la actualidad está desplazando a la tecnología IP/ATM, por su técnica de enrutamiento acelerado de paquetes, MPLS combina lo mejor de cada nivel (la inteligencia del routing con la rapidez del switching).

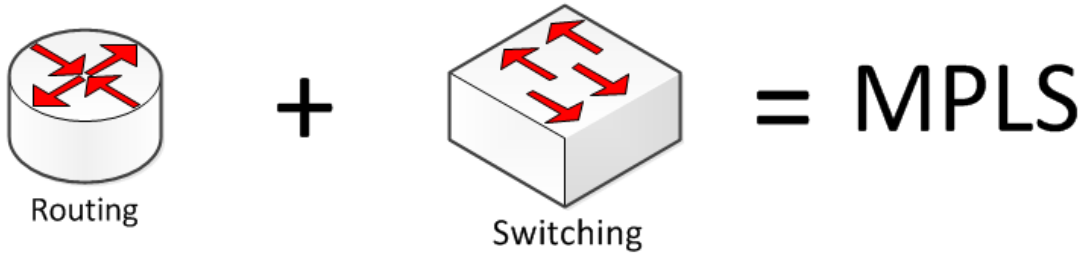

Figura 1. Combinación de MPLS

Algunos componentes, presentes en la red MPLS son los siguientes:

- Forwarding equivalance class FEC, permite describir los paquetes que tienen características comunes, como por ejemplo: IP origen, IP destino, puerto, QoS (véase anexo 1), etc.
- Routers de conmutación de etiquetas interior (LSR), enruta los paquetes en la red MPLS, la función principal que tiene es cambiar las etiquetas de los forwarding equivalence class, dependiendo como se encuentren en la tabla LIB.
- Routers de conmutación de etiquetas frontera de ingreso (LER de entrada), están al inicio de la red MPLS, su función es clasificar los paquetes de FECs y colocar las etiquetas.
- Routers de conmutación de etiquetas frontera de egreso (LER de salida), están en la salida de la red MPLS y eliminan la etiqueta del paquete MPLS, dejando el paquete en forma original.
- Protocolo de distribución de etiquetas (LDP), utilizan los LSRs para fijar las etiquetas.
- La base de información de las etiquetas (LIB), en el plano de control, asigna un prefijo IP a una etiqueta de significado local.
- La base de información del reenvío de etiquetas (LFIB), en el plano de datos, envía los paquetes basados en etiquetas para relacionar la

etiqueta deentrada con una interfaz de entrada y la etiqueta de salida con una interfaz de salida. (Salazar, 2015, pp. 8 -15)

En MPLS las etiquetas utilizan 32 bits, segmentados de la siguiente manera.

- 20 bits para las etiquetas (pero los 16 primeros bits están reservados).
- 3 bits para experimentación.
- 1 bit para stack, indicando el grupo de etiquetas.
- 8 bits para TTL, que permite eliminar los bucles en la red MPLS.

1.2.1 Características MPLS

Entre las características más importantes de la red MPLS son:

- Trabaja en la capa enlace y red del modelo OSI.
- Utiliza etiquetas para el marcado los paquetes y enrutar.
- Genera calidad de servicio dependiendo del etiquetado del paquete.
- Soporta múltiples protocolos como unicast, multicast, ingeniería de tráfico, QoS, VPN, etc.
- Soporta un MTU mayor a 1500
- Soporta diferentes redes como IP, ATM, Frame Relay, etc.

1.2.2 Funcionamiento

MPLS, es un método para reenvío de paquetes en una red utilizando información de las etiquetas añadidas a los paquetes IP, la asignación de etiquetas y su distribución es la siguiente:

Primero el protocolo de distribución de etiquetas LDP, establece vecindades entre LSRs, enviando frecuentemente mensajes de HELLO a las interfaces que hablan MPLS, las interfaces que han recibido el HELLO responden el mismo, permitiendo establecer adyacencias entre los routers, estos mensajes son difundidos en la red con la dirección multicast 224.0.0.2, utilizando el puerto 646 tanto en TCP y UDP.

Posteriormente los protocolos de enrutamiento (OSPF, EIGRP, IS-IS, etc.) construyen la tabla de enrutamiento IP, a cada ruta es asignada una etiqueta, la asignación y anuncios de las etiquetas es realizada por los LSR, cada LSR

tiene su propia base LIB, LFIB y FIB encontrándose en estas bases todas las etiquetas locales y las intercambiadas entre LSR.

Los LSR de core son los encargados de intercambiar las etiquetas de entrada por las de salida, basándose en la LFIB de cada router, finalmente en la salida los router LSR, remueven la etiqueta y analiza la información de enrutamiento para el envío del paquete Ip (Salazar, 2015, pp. 19 -24).

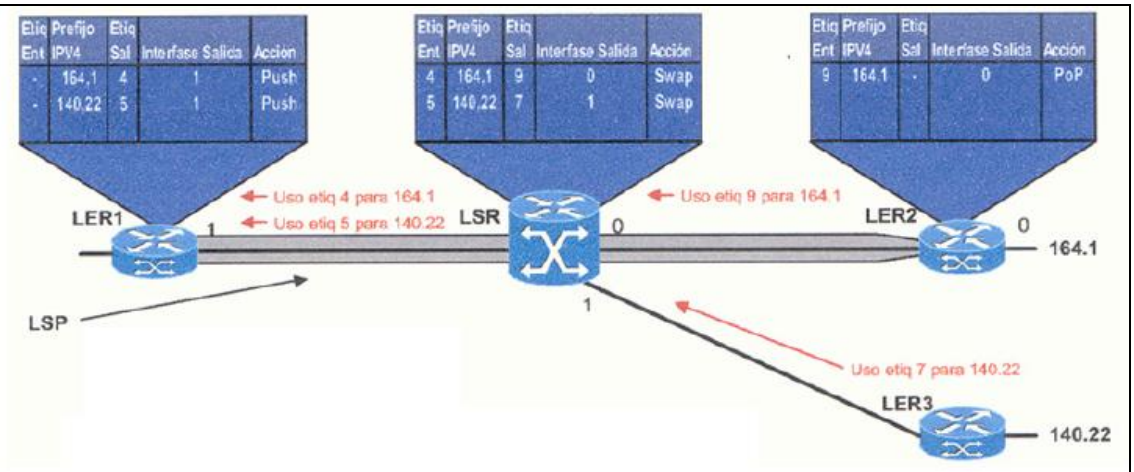

Figura 2. Funcionamiento de MPLS
Tomado de (Salazar, 2015, pp. 15)

1.2.3 Ventajas

- Escalabilidad en la red.
- Permite calidad de servicio QoS.
- Se puede crear clases de servicios.
- El ruteo es más rápido en el router de borde.
- Es una red de nueva generación.
- Soporte multiservicios.
- Garantiza un MTU mayor a 1500.
- Mejor desempeño en el reenvío de paquetes.
- No permite lazos en la red.

1.2.4 Desventajas

- Todos los routers tienen que trabajar MPLS.
- Incremento de una nueva capa 2 ½ en el modelo OSI.

1.2.5 QoS

En la trama de las etiquetas MPLS, la calidad de servicio se encuentra definida en el campo experimental que tiene 3 bits, permitiendo ocho posibilidades para el mismo.

Por defecto los 3 bits del campo DSCP (véase anexo 1) (IP Precedence) de la cabecera IP son copiados al campo EXP de MPLS.

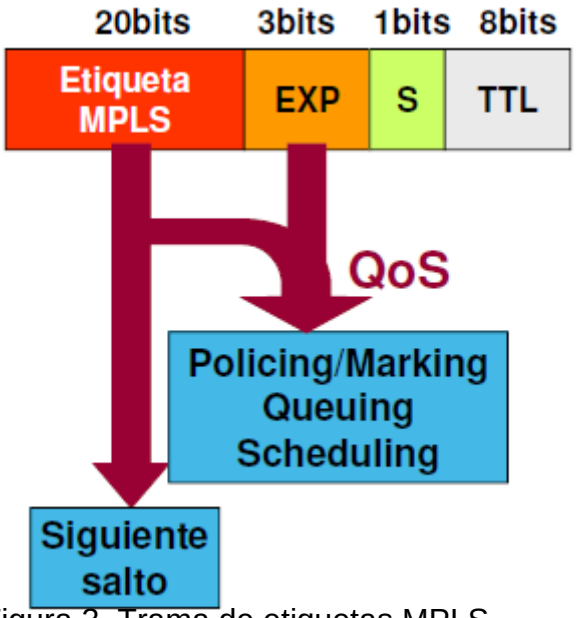

Figura 3. Trama de etiquetas MPLS

Tomoda de (cisco, s.f)

En los protocolos de distribución de etiquetas LDP, se garantizan los métodos de detección de lazos (loops) utilizados por los protocolos de Gateway interior que se usan para determinar el camino, pero si por configuraciones erróneas se generan lazos, el campo TTL sirve para minimizar los lazos infinitos. La propagación del TTL puede ser deshabilitada. En este caso el valor de TTL de la cabecera IP no es copiado en el campo TTL de la etiqueta y viceversa, se

coloca el valor inicial de 255 en el campo TTL de la etiqueta, también se puede deshabilitar la propagación del TTL entre los routers de core en el dominio MPLS (Salazar, 2015, pp. 4-19).

Inmediatamente se forma nuevas tablas de LFIB y FIB, basándose en la información que se encuentra en la base de datos de las etiquetas LIB.

1.2.6 Virtual Routing Forwarding VRF

Las VRF son empleadas para enrutamiento y envío de información de un grupo de subredes con idénticos requerimientos de conectividad, las VRF están relacionados generalmente por un route distinguisher (RD) y los router targer (RT) de import y export, estas VRF son asignadas a las interfaces físicas, loopback, subinterfaces y lógicas.

Cabe mencionar que cada interfaz solo soporta una sola VRF, pero la misma VRF puede estar configurada en muchas interfaces, también una interfaz puede no pertenecer a VRF alguna, sin embargo se puede recibir y enviar tráfico correspondiente a múltiples VPNs (véase anexo 1) por la misma interfaz esto se llama VRF selection usando PBR (véase anexo 1).

1.2.7 Router Distinguishers

EL RD es empleado para evitar duplicidad de direcciones de subred de los clientes, el router distinguishers expande los prefijos IP de cada dirección, consiguiendo tener un único prefijo que haga única a las direcciones IP de cada cliente, los prefijos está formado de 64 bits consiguiendo de esta manera una dirección IPv4 única de 96 bits que es suma de los 32 bits de una dirección IPv4 y los 64 bits de prefijo.

La dirección IP resultante es la dirección VPNv4. Las direcciones VPNv4 son intercambiadas entre los PE routers mediante BGP. El BGP que soporta otras familias de direcciones adicionales a las direcciones IPv4 es llamado Multiprotoco lBGP (MP-BGP). Generalmente MPLS VPN es usado dentro de un mismo sistema autónomo por lo que la sesión BGP entre los PE routers es siempre la sesión IBGP (Salazar, 2015, pp. 122). Generalmente el RD, en la configuración de un router solo lleva una línea la

cual es el número de sistema autónomo seguido de dos puntos y el número que diferencia las rutas.

Los router PE y LER (véase anexo 1) son de border, debido que están a los extremo de la red y ambos realizan etiquetado de los paquetes, pueden hablar multiples protocolos como MPLS, Ethernet.

1.2.8 Route-target RT

En ciertas redes la función de los router distinguishers no es suficiente para clasificar las redes por tal motivo se emplea los router target permitiendo participar en más de una red privada virtual, soportando topologías complejas.

Los route target son atributos adicionales adjuntos a las rutas BGP VPNv4 para indicar la participación en una VPN, dentro de BGP se utilizan las comunidades extendidas para codificar estos atributos, cualquier número de RTs pueden ser añadidos a una simple ruta. (Salazar, 2015, pp. 125)

Los route target existen de importación y exportación de prefijos cumpliendo las siguientes funciones.

Export RTs:

- Permite identificar la participación de cada red privada virtual
- Agrega rutas al convertirse en prefijos VPNv4

Import RTs:

- Asociados a cada tabla de enrutamiento virtual
- Elige las rutas que se van a implantar en tabla de enrutamiento virtual

1.2.9 VRF LITE

Es un servicio exclusivo de MPLS fundamentado en VRF (véase anexo 1), VRF-lite soporta múltiples VRFs con distintas tablas de enrutamiento y direccionamiento dentro de un mismo router, con VRF lite puede ser configurado en cualquier marca de router así estos no trabajen con MPLS y también soporta distintos protocolos de enrutamiento como EIGRP, OSPF, BGP, etc.

Las ventajas de utilizar VRF lite es que se tiene menor punto de falla en la red al igual que los costos de equipos físicos, debido que en un router se puede tener varias VRF es decir varios routers virtuales. (Salazar, 2015, pp. 129)

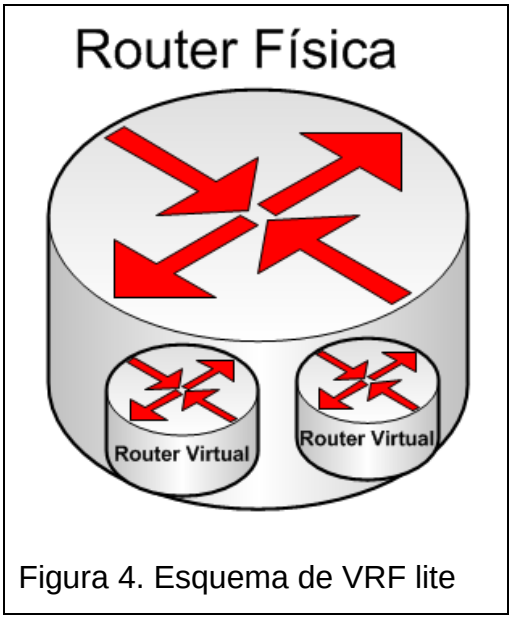

Figura 4. Esquema de VRF lite

El proceso de comunicación dentro de la red MPLS entre los router de borde del cliente CE, router de border del proveedor PE y router de core o backbone P es el siguiente:

1. El CE envía una actualización de enrutamiento IPv4 al PE.
2. El PE coloca un RD de 64 bits a la actualización de enrutamiento IPv4 obteniendo un prefijo único VPNv4.
3. El prefijo VPNv4 se propaga a través de la sesión MP-IBGP a los otros PE
4. El PE recibe la VPNv4 retira el RD obteniéndose nuevamente el prefijo IPv4.
5. Este prefijo es enviado al CE dentro de la actualización del enrutamiento IPv4.

1.3 IPV6

La habilidad para escalar las redes, para las demandas futuras requiere un suministro amplio de direcciones IP, la mejora de IPv6 es una cabecera más eficiente para satisfacer las actuales demandas.

Actualmente el Internet ha incrementado numerosamente, por ende, existen muchos dispositivos que demandan de una dirección IP, por ejemplo celulares, reproductores blue ray, TV, etc., esto está causando el agotamiento de las direcciones públicas IPv4 (mahidol, 2015, pp.10 - 18).

Para abordar el agotamiento de las direcciones las redes IPv4 utilizan NAT (véase anexo 1), pero esto puede causar problemas porque oculta la dirección de origen.

1.3.1 Características de las direcciones IPv6

- Son de 128 bits
- Se asignan mayor número de direcciones a comparación de IPV4.
- Se elimina el NAT
- Comunicaciones punto a punto son posibles
- Eliminación de direcciones broadcast
- Incluye direcciones unicast, multicast y anycast
- Soporte de movilidad y seguridad
- La cabecera se ha simplificado para mejorar la eficiencia del router
- Una interfaz de IPV6 puede tener varias direcciones
- No es necesario DHCP (véase anexo 1), ya que, los dispositivos IPV6 pueden asignar por si mismo una dirección de enlace único.

1.3.2 Cabecera IPV6

La principal característica en la cabecera de direcciones IPv6 es el nuevo campo para las etiquetas.

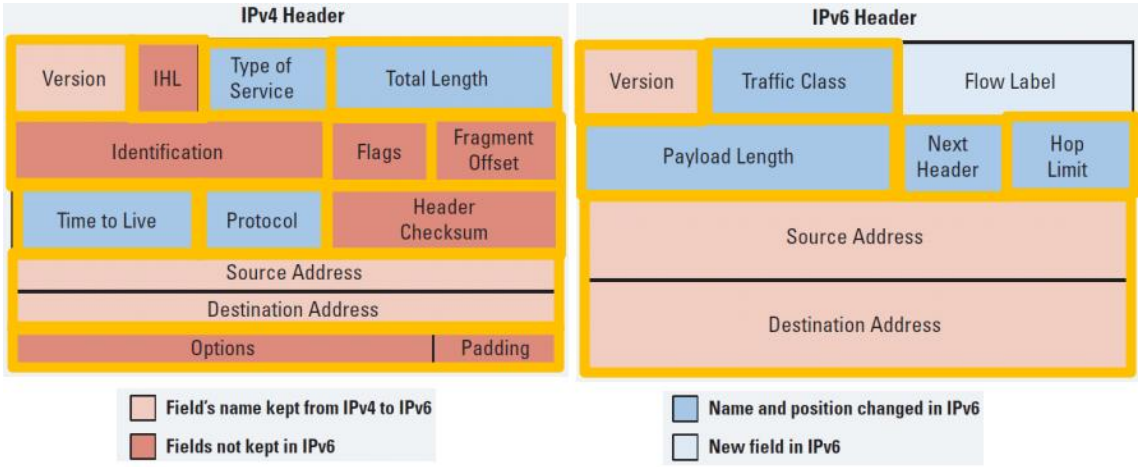

Figura 5. Comparación de las cabeceras IPV4 vs IPV6

Tomado de (mahidol, s.f)

a) Se observa que varios campos han sido modificados su nombre pero cumplen la misma función.

Las cabeceras de extensión tienen el campo dirección de destino:

Protocolos:

- TCP (protocolo de 6)
- UDP (protocolo 17)
- ICMPv6 (protocolo 58)
- Extensión de cabecera

IPV6 reemplazará gradualmente a IPV4, las dos versiones se configurarán y se ejecutarán de manera simultánea en la interfaz.

1.3.3 Direccionamiento IPV6

IPV6 aumenta el número de bits por un factor de 4, es decir, 128 bits, también estos se escriben con número hexadecimales.

Se compone de 8 segmentos de 16 bits separados por dos puntos (:), los dígitos hexadecimales no distinguen entre mayúsculas y minúsculas, por ejemplo: 2035:0001:2BC5:0000:0000:087C:0000:000A

Las abreviaturas para escribir un número hexadecimal es:

- Si inicia con 0, se pueden omitir, 09C0 = 9C0 y 0000 = 0.

- Un par de dos puntos (::) se puede utilizar dentro de una dirección, para representar cualquier número de 0 sucesivos. (mahidol, 2015, pp.25 - 34)

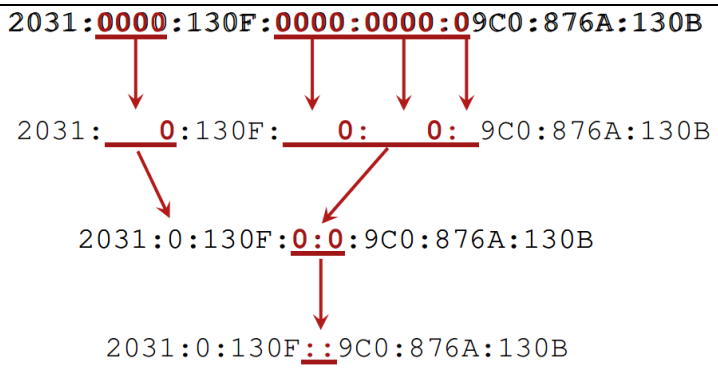

Figura 6. Ejemplos de abreviaturas con números hexadecimales

Tomado de (mahidol, s.f)

Una dirección IPV6 consta de dos partes:

Un prefijo de subred que representa la red, de 64 bits de longitud y un ID de interfaz llamado identificador local o token, también su longitud es de 64 bits.

Las direcciones IPv6 en un enlace deben ser únicas.

Los tipos de direcciones de destino tienen ámbitos bien definidos:

• Dirección de enlace local: se utilizan para la configuración automática de direcciones, como también, el descubrimiento de los vecinos por medio de varios protocolos.

• Dirección unicast global

La seguridad se basa en el protocolo Direcciones IPec, incluye encabezados de autenticación y extensión de encabezados, dicho protocolo asegura la comunicación de extremo a extremo.

1.4 BORDER GATEWAY PROTOCOL BGP

BGP es un protocolo de Gateway exterior EGP que advierte, aprende y elige la mejor ruta a nivel mundial, los ISP utilizan BGP para anunciar sus redes a nivel global, BGP cuenta con un algoritmo robusto que calcula la mejor ruta con la métrica más baja.

En la actualidad es uno de los protocolos de enrutamiento más populares con la versión 4 BGPv4, BGP no necesita indicar prefijos IPv4 como los protocolos de Gateway interior OSPF o EIGRP, únicamente necesita difundir determinada información entre todos los router vecinos para seleccionar la mejor ruta, en BGP los routers no tienen que estar físicamente juntos o en la misma subred para formar una vecindad basta que existe conectividad entre los equipos.

El protocolo BGP intercambia información de enrutamiento BGP por medio de actualizaciones de rutas llamadas atributos de ruta (AP), empleando el puerto TCP 179, utiliza la información de accesibilidad de la capa de red para determinar el prefijo IP y la longitud. (Salazar, 2015, pp. 356)

Una vez establecida la conexión TCP, los routers intercambian sus tablas de enrutamiento BGP completo. Sin embargo, debido a que la conexión es segura, los routers BGP necesitan enviar sólo las actualizaciones recientes, generalmente las actualizaciones de enrutamiento continúas no son necesarias en un enlace confiable, por lo que BGP envía mensajes keepalive, similar a los mensajes de saludo enviado por OSPF, IS-IS, y EIGRP.

Los atributos de ruta AP realizan tres procesos esenciales:

- Definen la información sobre una ruta en la red.
- Describe la información para la mejor ruta.
- Permite seleccionar la mejor ruta.

BGP, como método de contingencia, si no está presente el AP, procede a utilizar la ruta del sistema autónomo as_path para elegir la mejor ruta entre muchos router, también existe otras métricas como la preferencia local, peso, etc.

BGP realiza el siguiente proceso para seleccionar la mejor ruta o camino.

- La ruta con mayor peso (weight)
- La ruta con mayor preferencia local (local_pref)
- La ruta generada localmente
- El camino más corto (as_path)
- La ruta con el origen más bajo, es decir las rutas IGP, EGP e incompletas.
- La ruta que tenga el más bajo atributo discriminador de salida (MED)
- Las rutas de EBGP sobre las de IBGP
- La ruta del vecino IGP más cercano.
- La ruta más antigua de EBGP.
- La ruta del vecino BGP con valor del ID más bajo.
- La ruta del vecino BGP con la IP más baja.

1.4.1 IBGP

Cuando dos routers se encuentran en un mismo sistema autónomo se establece un IBGP, una de las características de IBGP es que todos los router tienen la misma información de la tabla de enrutamiento, necesario para posibles publicaciones de rutas con los EBGP.

Se deben establecer los siguientes requerimientos para considerar un IBGP.

- Tienen que tener el mismo sistema autónomo.
- Establecer una sesión TCP entre routers.
- Tiene que ser alcanzables entre routers.

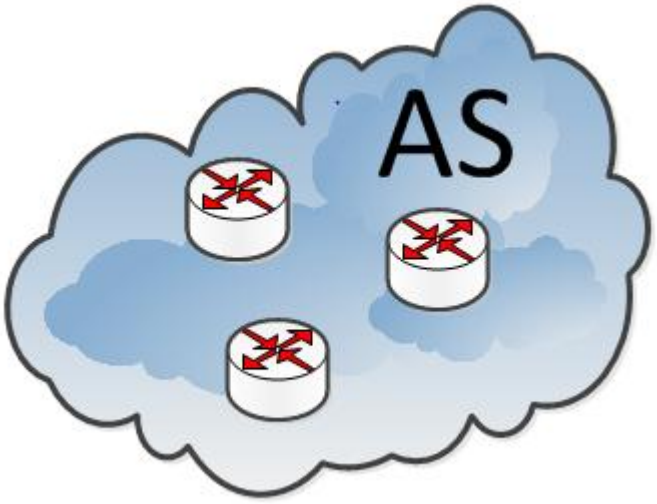

Figura 7. Vecinos IBGP

Cabe mencionar que los router no tienen que estar conectados directamente basta que tengan conectividad entre ellos, se emplea las vecindades para no generar posibles lasos en la red.

IBGP no es protocolo de tránsito por las siguientes características:

- No transita las rutas de un sistema autónomo externo.
- Las redes empresariales son de no tránsito.
- Todos los router, aunque no sean de tránsito, deben tener las rutas externas.
- Las rutas aprendidas por IBGP no son publicados a otros vecinos IBGP.

1.4.2 EBGP

El protocolo de Gateway de borde externo EBGP, es empleado entre routers que se encuentren en diferentes sistemas autónomos AS, es decir, los vecinos están en un sistema autónomo diferente, los protocolos de Gateway interior no funcionan en EBGP.

Dos routers para intercambiar información de enrutamiento BGP, establecen tres vías antes de inicializar la sesión BGP. Por lo tanto, la dirección IP utilizada en el router vecino debe ser accesible sin necesidad de utilizar un IGP,

esto puede ser realizada por enrutamiento a una dirección que se puede alcanzar a través de una red conectada directamente o rutas estáticas a esa dirección IP, generalmente están conectadas directamente.

Las empresas tienen conexiones con varios proveedores de internet ISP, al igual que los ISP tienen enlaces con diferentes proveedores de internet, todas estas conexiones trabajan en diferentes sistemas autónomos por tal motivo se requiere sesiones EBGP entre routers.

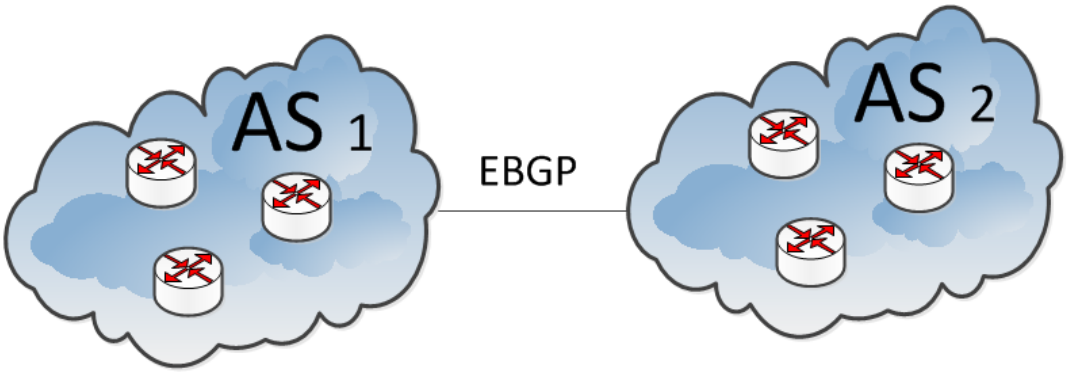

Figura 8. Vecinos EBGP

EBGP estable los siguientes requerimientos para poder establecer una vecindad

- Los routers tienen que estar en diferente sistema autónomo.
- Establecer una sesión TCP entre los routers.
- Tener conectividad entre las direcciones IP de los routers.

1.4.3 Sistema Autónomo AS

El sistema autónomo es un conjunto de router que están bajo un mismo dominio administrativo y similares políticas de enrutamiento, es decir, en un protocolo de Gateway interior IGP, para establecer comunicación con otros sistemas autónomos se realiza mediante un protocolo de Gateway exterior EGP (redes-linux, s.f, p.3).

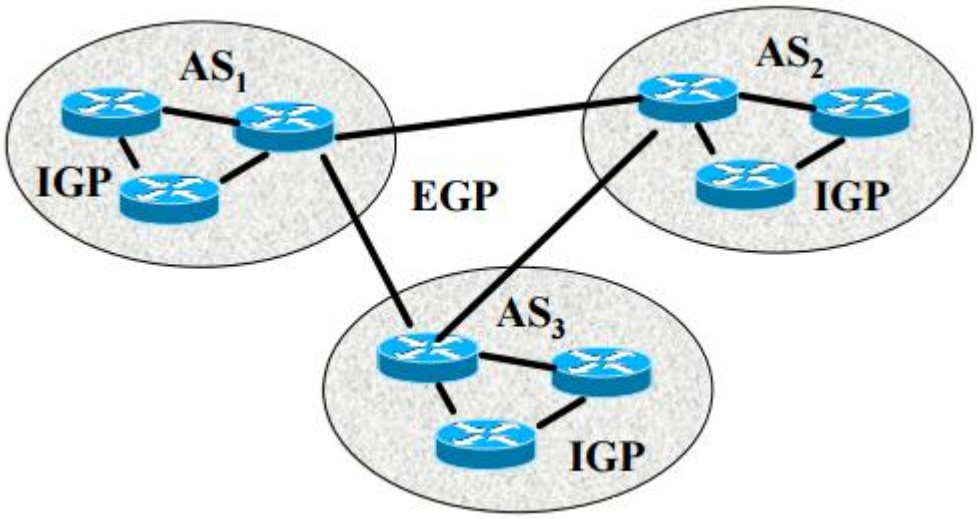

Figura 9. Sistema Autónomo
Tomado de (redes-linux, s.f)

El sistema autónomo esencial para el funcionamiento de BGP, los sistemas autónomos son identificados por un número entero decimal desde 1 hasta 65635, tiene una similitud con las direcciones IPv4 debido que existe sistemas autónomos públicos en el rango desde 1 hasta 64511 y los sistemas autónomos privados que va desde 64512 hasta 65535

1.4.4 Base de datos BGP

La base de datos del protocolo está constituida en tres partes:

Base de datos de vecinos

- Lista de vecinos BGP

Base de datos para reenviar rutas

- Lista de todas las redes aprendidas de cada vecino
- Puede contener varias rutas de acceso a las redes de destino
- Contiene los atributos BGP para cada ruta

Base de datos de enrutamiento IP

- Lista de las mejores rutas de acceso a las redes de destino

1.5 OBSERVIUM

Es un sistema de monitoreo, que permite identificar automáticamente los terminales que están conectados a una red como son: servidores, routers, switchs, etc., también reconoce sistemas operativos incluyendo Windows, Linux, etc., está basado en PHP/MySQL, es decir, se puede acceder a una base de datos desde PHP (Lenguaje de código abierto conveniente para el desarrollo web). Existen dos tipos de sistemas Observium, estos son:

Comunidad: es gratuito, presenta características básicas con ciertas limitaciones, se distribuye a través de la licencia QPL Open Source.

Profesional: es un software pagado que ofrece varias características, entre una de ellas es el soporte y otros servicios disponibles, necesita diferentes parches y una licencia anual (cioperu, s.f).

1.5.1 Características

El software profesional proporciona actualizaciones de seguridad a tiempo real y también nuevas características como es el tráfico de contabilidad, es decir, es una característica que facilita el control y la facturación del ancho de banda del cliente.

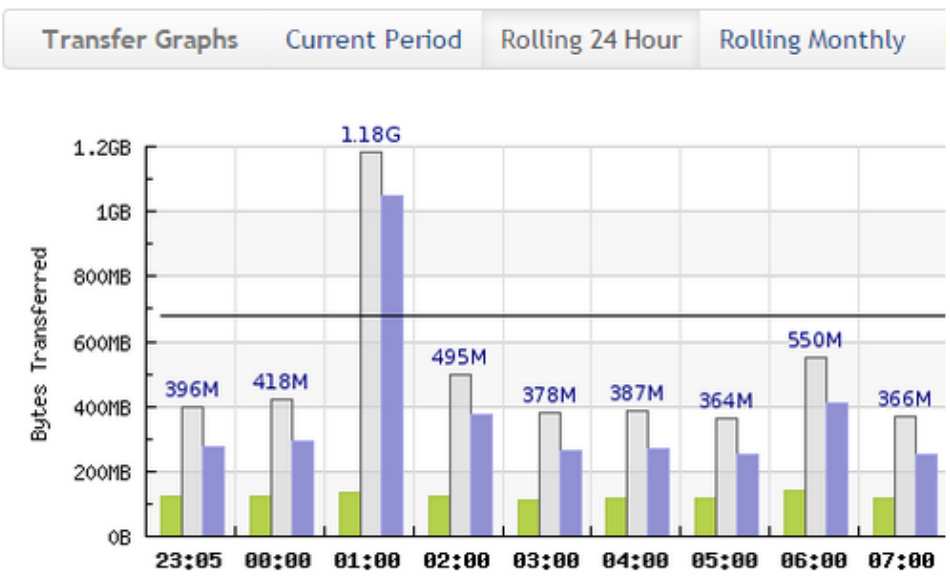

Figura 10. Esquema de VRF lite

Recuperada de (Observium, s.f).

Otra característica interesante es la integración externa, es decir, es la integración con varias aplicaciones de terceros para obtener reportes óptimos y más específicos (cioperu, s.f).

También, tiene la alerta umbral, es decir, admite configurar umbrales y los estados de fallo de los diferentes dispositivos conectados en la misma red.

Es un sistema fácil de instalar y configurar, se puede ingresar por medio de una interfaz gráfica amigable para el usuario en donde indica variedad de estadísticas, gráficas y tablas con información sobre cómo está trabajando la red (pceuador, s.f, p. 27-38).

1.5.2 Ventajas

Entre las ventajas que presenta un sistema de monitoreo observium son:

- Es fácil su administración
- No existe limitación de dispositivos en una red, el descubrimiento es automático.
- Soporta una extensa gama de sistemas operativos y hardware.
- Mapea la red por medio de protocolos de descubrimiento
- Reconocimiento automático de dispositivos
- Proporciona información para actuar proactivamente con ciertos problemas antes que el servicio se vea afectado.
- Mejora la visibilidad de la infraestructura de la red.
- Es monitor de host, puede escanear el rango de direcciones IPv4 e IPv6.

1.5.3 Desventajas

- No es un sistema de alarmas en ciertos eventos de servidores y servicios.
- Es solo una herramienta vía web para mostrar ciertos datos como el estado de los servidores.
- No es interactivo.
- Al utilizar el software gratuito existen varias limitaciones, como por ejemplo el sistema de contabilidad de tráfico.

2. Capítulo II. Análisis y Diseño De la RED

2.1 Topología actual de la red

En la actualidad la empresa Urbano Express cuenta con 41 enlaces a nivel nacional y concentradores en Quito, Guayaquil y Cuenca, con servicios de datos e internet, provistos por PUNTONET, cada enlace tiene redundancia en la última milla con excepción de determinados puntos, los enlaces principales generalmente son conexiones de fibra óptica y los de respaldo (backup) son radio enlaces, ADSL y VSAT. En ciertos lugares por cobertura no se llega con la infraestructura propia del ISP (véase en anexo 1) Puntonet y se tiene subcontratado los enlaces de última milla de otros proveedores, pero los equipos de capa tres son instalados y administrados por Puntonet S.A, los equipos de capa dos son de la siguientes marcas: terminal de red óptico ONT: coreccess o Calix, radio: Mikrotik_Metal, módem ADSL: Tp-link y módem VSAT: iDirect, los router de capa son Cisco o Mikrotik.

Para la conmutación de enlace principal a enlace de backup, se emplea rutas estáticas con una métrica mayor, protocolos de enrutamiento dinámicos OSPF o EIGRP, todos los enlaces tiene un conjunto (pool) de direcciones IP públicas, con una máscara de treinta o veinte y nueve bits. Para comunicarse con las matrices cada sucursal emplea túneles, o protocolos como GRE (véase anexo 1) y otros de VPN sobre internet.

La restricción del ancho de banda se realiza generalmente en la última milla en capa dos, aunque en determinadas sucursales se implementa la limitación en las interfaces de los router de capa tres, en estos router también se configura listas de acceso para restringir y permitir la navegación a destinos específicos.

2.1.1 Topología actual de la matriz

Concentrador datos Quito

Como se muestra en la figura No. 11, el concentrador principal, ubicado en la ciudad de Quito, tiene la última milla con fibra óptica con un ONT marca corecess y el backup con radio enlace, el ancho de banda del enlace principal

es de 47 Mbps compartición uno a uno, tiene una subred de direcciones IP privada con máscara de treinta bits, utilizadas como IP de enlace entre el router concentrador CE y el router de border de Puntonet PE, en el PE se tiene configurada la ip en una interfaz vlan y en el CE en una interfaz Fastethernet de capa 3. El enlace de backup es de 25 Mbps al igual que el principal tiene ip de enlaces y vlan para establecer la comunicación entre CE y PE, el protocolo de enrutamiento a nivel WAN (véase anexo 1) para una conmutación automática es EIGRP.

En el router principal se emplea dos direcciones IP públicas configuradas en interfaces loopbacks, utilizada para realizar los túneles hacia las siguientes sucursales Santo Domingo, Portoviejo, Milagro, La Libertad, Quevedo, Loja, Cayambe, Babahoyo, Esmeraldas, Coca, Guaranda, Lago Agrio, Tulcán, Ibarra, Puyo, Rio Coca UIO y a los concentradores de Guayaquil y Cuenca.

La conectividad de LAN a LAN entre matriz y sucursales se forma con rutas estáticas y enrutamiento dinámico EIGRP, internamente en la LAN de matriz se tiene un pool de direcciones privadas alcanzadas mediante el host 192.168.1.82.

Conserva un enlace hacia internet con un router cisco 1720 el cual sirve para VoIp con Guayaquil este enlace tiene 2 Mbps de ancho de banda y la última milla es fibra óptica corecess del puerto 100 TX.

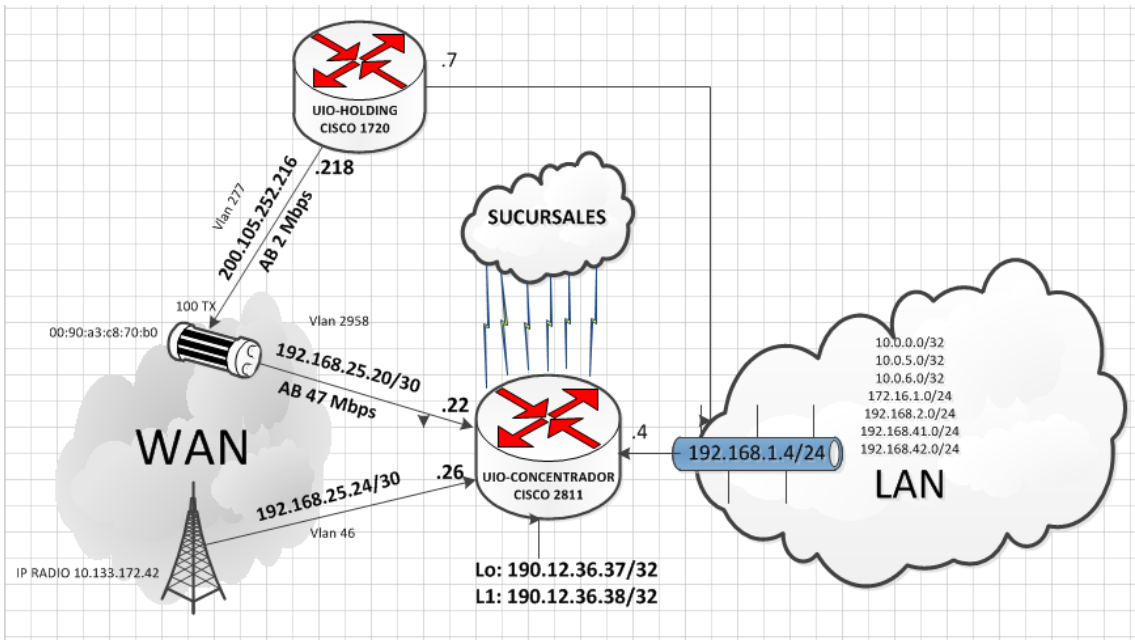

Figura 11. Topología del concentrador matriz Quito

Concentrador datos Guayaquil

Como se muestra en la figura No. 12, en la ciudad de Guayaquil, el concentrador de datos y acceso a Internet accede con la última milla de fibra óptica y radio enlace para el enlace de backup. Para la conmutación automática del backup, se emplea el protocolo de enrutamiento dinámico OSPF en un Mikrotik 2011, se tiene dos subredes privadas de enlace, con una máscara de treinta bits para la conectividad PE-CE con el principal y el enlace backup, el ancho de banda de es de 40 Mbps para datos, y 5 Mbps para acceso Internet.

El Mikrotik 2011 tiene dos pool de direcciones IP públicas /29, con un pool de ip pública se realiza la conexión al router cisco 1721, que es el concentrador de datos y tiene configurado los túneles GRE a las siguientes sucursales: Ibarra, Riobamba, Chone, Santo Domingo, Esmeraldas, Babahoyo, Latacunga, Puyo, Quevedo, Ambato, Milagro, Guaranda principal y backup, Salinas, Manta, Azogues, Coca, Tena, Portoviejo, Machala, Machala, Loja, Lago Agrio, Naranjal, Playas, Cayambe, Zamora, Santo Domingo Logística, Serpricarga

GYE y Quito, el otro segmento de direcciones IP públicas son administradas por el cliente para el enlace de internet.

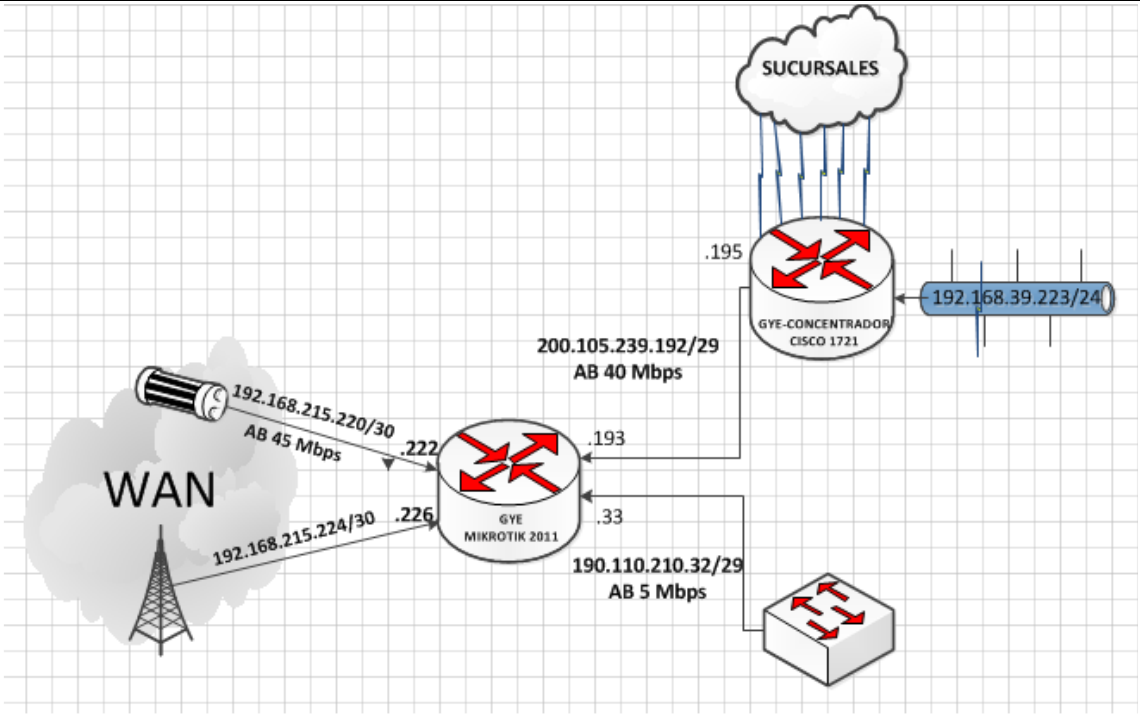

Figura 12. Topología del concentrador matriz Guayaquil

En la figura 13 se muestra la configuración de un router Mikrotik 2011, en el cual se tiene la dirección IP, los vecinos del protocolo OSPF, las interfaces y las colas de restricción del ancho de banda.

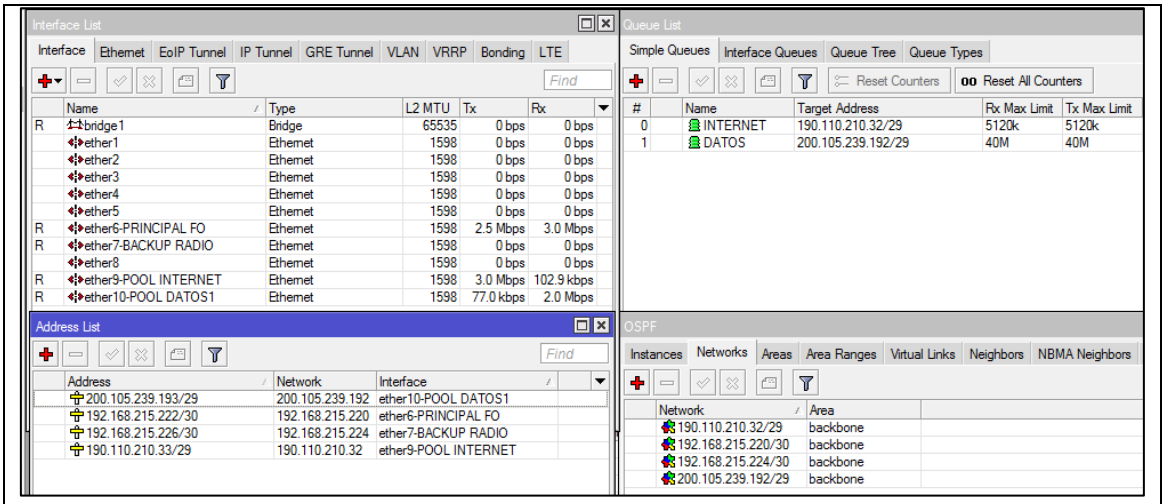

Figura 13. Configuración del Router OSPF Guayaquil

2.1.2 Topología actual de las sucursales

Sucursal Puyo

En la ciudad Puyo, como se muestra en la figura No. 14, la última milla del enlace principal es ADSL (provisto por CNT) y en enlace de backup es VSAT, dos rutas por defecto, configuradas con peso se utilizan para definir los enlaces principal y de backup, las subredes públicas son asignadas para el enlace WAN. Se comunica mediante túneles GRE hacia Guayaquil, Cuenca y Quito, en este último se posee dos túneles funcionado como principal y de backup de manera automática, mediante el protocolo EIGRP, el router instalado es un cisco 1751 que tiene tres interfaces.

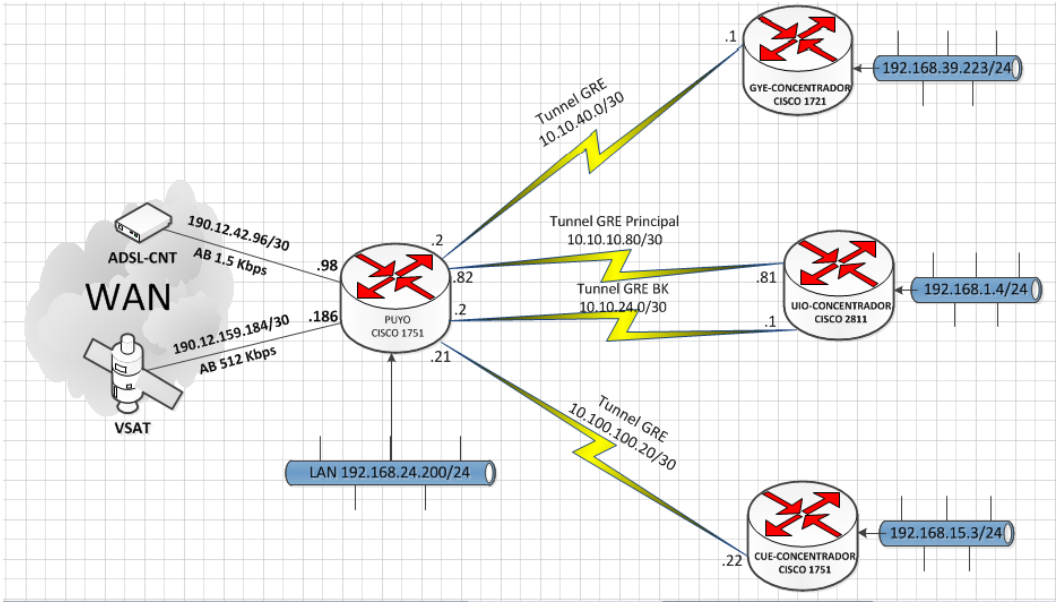

Figura 14. Topología sucursal Puyo

Sucursal Tena

En la ciudad Tena, como se muestra en la figura No. 15, la última milla del enlace principal es radio enlace y en enlace de backup es ADSL (provisto por CNT), dos rutas por defecto, configuradas con peso se utilizan para definir los enlaces principal y de backup, las subredes públicas son asignadas para el enlace WAN. Se comunica mediante túneles GRE hacia Guayaquil, Cuenca, Aceitunas y Quito, en este último se posee dos túneles funcionado como principal y de backup de manera automática, mediante el protocolo EIGRP, el router instalado es un cisco 1811 que tiene tres interfaces en donde está limitado el ancho de banda de 1.5 Mbps.

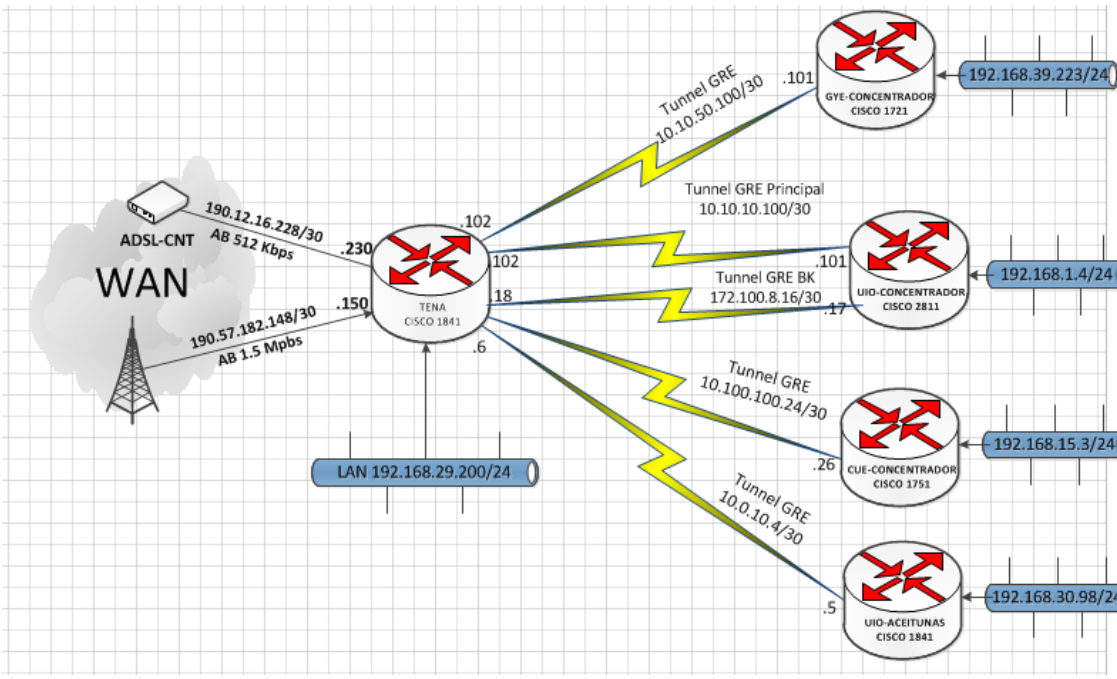

Figura 15. Topología sucursal Tena

Sucursal Esmeraldas

En la ciudad de Esmeraldas, como se muestra en la figura No. 16, la última milla del enlace principal es fibra óptica y el enlace de backup en radio enlace, a nivel de WAN tiene dos subredes privadas mascara de treinta bits que están en el proceso EIGRP para la conmutación del backup, también una subred pública mascará de treinta bits que permite la comunicación directa con el router de datos en el cual se tiene un tuneles GRE hacia Quito, el router_eigrp instalado es un cisco 1720 de tres interfaces en donde está limitado el ancho de banda de 2 Mbps, el router de datos es cisco 1751 de tres interfaces.

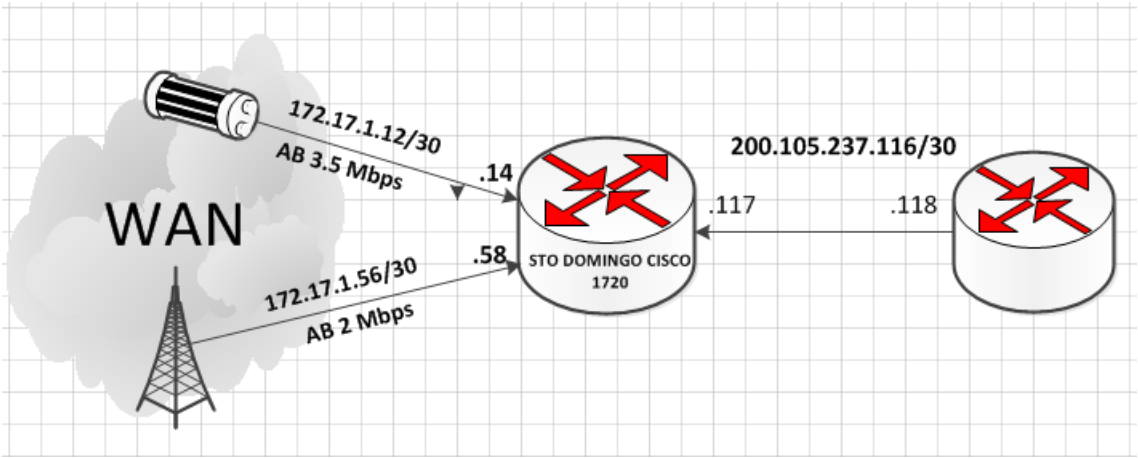

Figura 16. Topología sucursal Santo Domingo

Sucursal Riobamba

En la ciudad de Riobamba, como se muestra en la figura No. 16, la última milla del enlace principal con FO y backup con radio enlace, el primer router cisco 1751 funciona para recoger las dos ip de enlace y realizar la conmutación automática por el protocolo dinámico EIGRP, también está conectado directamente con el segundo router cisco 1751, en el cual se encuentran configurados los servicios de datos mediante tuneles GRE hacia Quito, Guayaquil y Logistecsa Quito, ancho de banda es de 3.5 Mbps.

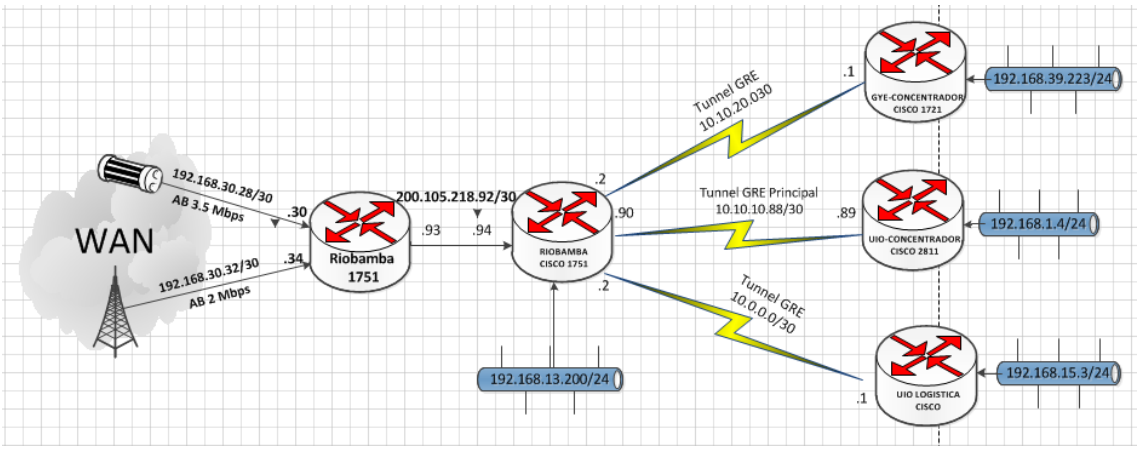

Figura 17. Topología sucursal Riobamba

2.1.3 Direccionamiento

La red actual, presenta una utilización elevada del direccionamiento de direcciones IP públicas, todas las sucursales tienen una subred pública mascara 30 o 29, empleadas para la configuración de los túneles GRE hacia la matriz, en determinados enlaces también se tiene subredes privadas como enlaces WAN.

En la tabla No.1 se detalla el direccionamiento IPv4 de direcciones públicas y privadas de todas las sucursales y la matriz.

Tabla 1. Direcciones IPv4 red Ethernet actual Urbano Express

#	Enlace	IP Wan principal	Ip Wan Backup	Ip Lan CE Eigrp	Wan CE Internet	LAN
1	Tena	190.57.182.150/30	190.12.16.230/30	NA	NA	192.168.29.200/24
2	Manta	172.29.1.6/30	172.29.1.94/30	190.12.14.189/30	190.12.14.190/30	192.168.4.223/24
3	Sto. Domingo	172.17.1.14/30	172.17.1.58/30	200.105.237.117/30	200.105.237.118/30	NA
4	Sucursal GYE	NA	NA	190.110.210.34/30	NA	NA
5	Renazzo	190.12.47.98/30	NA	NA	NA	200.105.246.105/30
6	Puyo	190.12.42.98/30	190.57.159.186/30	NA	NA	192.168.24.200/24
7	Tulcán	190.110.207.38/30	190.110.197.30/30	NA	NA	192.168.23.200/24
8	Loja	172.16.2.2/30	172.16.2.6/30	190.12.13.53/30	190.12.13.54/30	192.168.10.200/24
9	Cayambe	192.168.9.198/30	192.168.30.18/30	190.12.38.97/30	190.12.38.98/30	192.168.12.200/24
10	Chone	190.12.63.126/30	NA	NA	NA	192.168.25.200/24
11	Libertad	190.110.223.18/30	NA	NA	NA	192.168.6.230/24
12	Babahoyo	192.168.208.86/30	192.168.208.82/30	NA	190.12.53.66/30 190.57.128.90/30	192.168.14.200/24 192.168.14.252/24
13	Lago Agrio	192.168.14.246/30	NA	190.12.41.81/30	190.12.41.82/30	192.168.30.200/24
14	Ambato	192.168.20.58/30	192.168.20.54/30	190.110.219.253/30	190.110.219.254/30	192.168.16.200/24

15	Guaranda	192.168.12.142/30	NA	190.12.34.121/30	190.12.34.122/30 190.110.194.126/30	192.168.19.200/24
16	Riobamba	192.168.30.30/30	192.168.30.34/30	190.110.218.93/30	190.110.218.94/30	192.168.13.200/24
17	Ibarra	192.168.50.38/30	192.168.50.42/30	190.110.206.29/30	190.110.206.30/30	192.168.17.10/24
18	Esmeraldas	190.110.201.26/30	190.110.194.122/30		NA	192.168.11.200/24
19	Latacunga	192.168.20.130/30	192.168.20.186/30	190.57.173.73/30	190.57.173.74/30	192.168.18.200/24
20	Portoviejo	190.57.176.54/30	190.12.14.186/30	NA	NA	192.168.3.200/24
21	Quevedo	190.12.29.186/30	NA	NA	NA	192.168.9.200/24
22	Milagro	190.12.2.142/30	NA	NA	NA	192.168.8.200/24
23	Quito Internet	192.168.21.6/30	192.168.0.6/30	NA	NA	192.168.12.189/30 190.12.42.81/29 200.105.232.204/30 200.105.232.249/29
24	Gye Internet	NA	NA	200.105.239.193/29	NA	190.110.210.33/29
25	Holding	192.168.12.34/30	NA	NA	NA	190.12.47.113/30
26	Cuenca	192.168.48.170/30	192.168.48.146/30	190.12.4.181/30	190.12.4.182/30	192.168.15.3/24
27	Machala	192.168.100.34/30	192.168.100.30/30	NA	NA	190.12.56.198/30 192.168.5.223/24
28	Coca	190.110.222.30/30	NA	NA	NA	192.168.27.200/24

29	Zamora	192.168.22.118/30	NA	190.110.194.189/30	190.110.194.190/30	192.168.33.200/24
30	Gye Datos	200.105.239.195/29	NA	NA	NA	192.168.39.223/24
31	Quito Datos	192.168.25.22/30	192.168.25.26/30	NA	NA	192.168.1.4/24
32	Naranjal	192.168.13.106/30	NA	190.12.39.190/30	190.12.39.189/30	192.168.7.200/24
33	Bahia	192.168.28.78/30	NA	190.12.46.133/30	190.12.46.134/30	192.168.21.200/24
34	Azogues	192.168.43.46/30	192.168.48.166/30	190.110.216.137/30	190.110.216.138/30	192.168.20.3/24
35	Granados	NA	NA	NA	192.168.1.82	192.168.42.200/24
36	Playas	NA	NA	190.12.3.65/30	190.12.3.66/30	192.168.31.200/24
37	Macas	NA	NA	190.57.179.45/30	190.57.179.46/30	192.168.28.200/24
38	Tulipanes	NA	NA	NA	192.168.1.82	192.168.41.200/24

Tabla 2. Direccionamiento IPv4 red Ethernet actual Serpricarga

	SEPRICARGA	**IP Wan principal**	**Ip Wan Backup**	**Ip Lan router Eigrp**	**Wan R Internet**	**LAN**
1	**Sto. Domingo**	NA	NA	NA	200.105.255.246/30	192.168.53.200/24
2	**Portoviejo**	NA	NA	NA	190.57.176.182/30	192.168.51.200/24
3	**Guayaquil**	NA	NA	NA	190.57.128.170/30	197.1.2.160/26
4	**Quito**	192.168.17.134/30	192.168.30.98/30	NA	NA	190.12.12.97/30 197.1.2.126/25 190.57.155.173/30

2.1.4 Enrutamiento

En las matrices y sucursales, las tablas de enrutamiento son complejas, difíciles para brindar un soporte en el momento que presente un error en la red o falta de conectividad en determinados enlaces.

En la figura No. 18 a continuación se muestra una parte de la tabla de rutas del concentrador en la ciudad de Quito:

```
URBANOEXPRESSMATRIZCONCENTRADORDATOS#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.25.21 to network 0.0.0.0

S     192.168.12.0/24 [1/0] via 10.10.10.46
D     192.168.29.0/24 [90/14075392] via 10.10.10.102, 01:49:14, Tunnel20
S     192.168.28.0/24 [1/0] via 10.100.200.2
S     192.168.13.0/24 [1/0] via 10.10.10.90
S     192.168.14.0/24 [1/0] via 10.10.14.2
S     192.168.31.0/24 [1/0] via 10.100.200.6
                      [1/0] via 10.0.0.1
S     192.168.30.0/24 [1/0] via 10.5.0.2
S     192.168.15.0/24 [1/0] via 10.100.100.2
S     192.168.60.0/24 [1/0] via 172.100.8.30
S     192.168.42.0/24 [1/0] via 192.168.1.82
S     192.168.8.0/24 [1/0] via 10.10.10.18
      192.168.25.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.25.20/30 is directly connected, FastEthernet0/1
C        192.168.25.24/30 is directly connected, FastEthernet0/0
S        192.168.25.0/24 [1/0] via 10.10.10.106
D     192.168.24.0/24 [90/13635840] via 10.10.10.82, 01:49:14, Tunnel16
S     192.168.9.0/24 [1/0] via 10.10.10.34
      190.12.0.0/32 is subnetted, 2 subnets
C        190.12.36.38 is directly connected, Loopback1
C        190.12.36.37 is directly connected, Loopback0
S     192.168.10.0/24 [1/0] via 10.10.10.42
S     192.168.27.0/24 [1/0] via 10.10.10.98
      172.100.0.0/30 is subnetted, 8 subnets
C        172.100.8.0 is directly connected, Tunnel68
C        172.100.8.4 is directly connected, Tunnel69
C        172.100.8.8 is directly connected, Tunnel70
C        172.100.8.12 is directly connected, Tunnel71
C        172.100.8.16 is directly connected, Tunnel72
C        172.100.8.20 is directly connected, Tunnel76
C        172.100.8.24 is directly connected, Tunnel78
C        172.100.8.28 is directly connected, Tunnel79
      172.16.0.0/24 is subnetted, 1 subnets
S        172.16.1.0 [1/0] via 192.168.1.82
S     192.168.26.0/24 [1/0] via 10.10.10.66
D     192.168.11.0/24 [90/14075392] via 10.10.10.62, 01:49:14, Tunnel8
S     192.168.41.0/24 [1/0] via 192.168.1.82
S     192.168.200.0/24 [1/0] via 10.10.200.2
S     192.168.4.0/24 [1/0] via 10.10.200.2
S     192.168.21.0/24 [1/0] via 10.10.10.70
S     192.168.39.0/24 [1/0] via 10.0.0.1
S     192.168.20.0/24 [1/0] via 10.10.10.94
S     192.168.5.0/24 [1/0] via 10.10.10.114
      10.0.0.0/8 is variably subnetted, 44 subnets, 2 masks
```

Figura 18. Ruta matriz Quito red Ethernet actual

2.1.5 Equipos

En la matriz y en la mayoría de las sucursales existe un dimensionamiento erróneo de los equipos, causando una pérdida económica proveedor de

servicio de internet ISP, debido que en la forma en la que se encuentran operando e instalados los equipos en la actualidad, no ofrecen una redundancia a la red ni escalabilidad, pese que se utiliza uno o dos router de buenas prestaciones, por el costo de adquisición de cada router al ISP representa una pérdida, debido que el ISP instala los equipos a modo de préstamo mientras el servicio se encuentre activo, es decir, este gasto es adquirido por el ISP, por ejemplo en la sucursal de Riobamba se puede evidenciar en la topología obtenida que utiliza dos equipos físicos de capa 3 que son dos router cisco de 1751 cada uno de estos router tiene 3 interfaces de capa 3 y la posibilidad de una WIC2H(véase anexo 1).

El ISP maneja un gama de equipos terminales para el cliente tanto de capa 3 como de capa 2, por ejemplo router Cisco o Mikrotik, módem de marca iDirect para la plataforma satelital, módem TP-link para los enlaces ADSL, a nivel de fibra óptica marcas como coreccess y Calix.

2.2 Diseño de la red en MPLS

Con la información recopilada de topología, direccionamiento, enrutamiento y equipos de los 41 enlaces a nivel nacional tanto de internet como datos, se procede a diseñar cada uno de los enlaces en la red MPLS.

En la empresa Urbano Express, para los enlaces de matriz Quito y Guayaquil, se instalará un router cisco que será virtualizado con la técnica de VRF LITE, para proveer los servicios de datos e internet en un solo equipo, el protocolo de red será BGP a nivel de la WAN para la conmutación automática de los enlaces de backup. En Quito se tendrá el enlace principal y de backup a nivel de la última milla con fibra óptica, en Guayaquil el enlace principal será fibra óptica y el backup radio enlace. Estos equipos serán instalados en paralelo para no afectar los servicios actuales con el resto de las sucursales.
Las sucursales serán migradas con el respectivo cronograma, se instalará un router Cisco o Mikrotik de tres interfaces con el protocolo BGP a nivel de la WAN, la salida al internet será a través de la matriz Quito o Guayaquil. Las prioridades de salida al internet tendrá el siguiente orden: internet principal Quito, internet backup Quito, internet principal Guayaquil o internet backup Guayaquil, esta prioridad se designa mediante el atributo BGP denominado

“as_path”, a fin de obtener una redundancia alta para la salida al internet de cada sucursal.

2.2.1 Direccionamiento IPv4

Para los enlaces de datos en las sucursales y matriz se designarán dos subredes privadas mascara de treinta bits, empleadas para el enlace WAN entre el PE y CE, la primer subred es para el enlace principal, la IP impar será configurada en el PE y la IP par será configurada en el CE, la segunda subred estará designada para el enlace de backup. Los enlaces de internet de Quito, Guayaquil, Ranazo y Holding se asignará un subred de IP pública mascara de treinta bits.

El direccionamiento a nivel nacional será el indicado en la tabla No. 3.

Tabla 3. Direccionamiento Ipv4 red MPLS

Número	Enlace	WAN PRINCIPAL	WAN BACKUP
1	Quito Datos Concentrador	10.10.10.0/30	10.10.10.4/30
2	Gye Datos Concentrador	10.10.10.8/30	10.10.10.12/30
3	Cuenca	10.10.10.16/30	10.10.10.20/30
4	Tena	10.10.10.24/30	10.10.10.28/30
5	Manta	10.10.10.32/30	10.10.10.36/30
6	Sto. Domingo	10.10.10.40/30	10.10.10.44/30
7	Puyo	10.10.10.48/30	10.10.10.52/30
8	Tulcán	10.10.10.56/30	10.10.10.60/30
9	Loja	10.10.10.64/30	10.10.10.68/30
10	Cayambe	10.10.10.72/30	10.10.10.76/30
11	Chone	10.10.10.80/30	10.10.10.84/30
12	Libertad	10.10.10.88/30	10.10.10.92/30
13	Babahoyo	10.10.10.96/30	10.10.10.100/30
14	Lago Agrio	10.10.10.104/30	10.10.10.108/30
15	Ambato	10.10.10.112/30	10.10.10.116/30
16	Guaranda	10.10.10.120/30	10.10.10.124/30
17	Riobamba	10.10.10.128/30	10.10.10.132/30

18	Ibarra	10.10.10.136/30	10.10.10.140/30
19	Esmeraldas	10.10.10.144/30	10.10.10.148/30
20	Latacunga	10.10.10.152/30	10.10.10.156/30
21	Portoviejo	10.10.10.160/30	10.10.10.164/30
22	Quevedo	10.10.10.168/30	10.10.10.172/30
23	Milagro	10.10.10.176/30	10.10.10.180/30
24	Machala	10.10.10.184/30	10.10.10.188/30
25	Coca	10.10.10.192/30	10.10.10.196/30
26	Zamora	10.10.10.200/30	10.10.10.204/30
27	Naranjal	10.10.10.208/30	10.10.10.212/30
28	Bahia	10.10.10.216/30	10.10.10.220/30
29	Azogues	10.10.10.224/30	10.10.10.228/30
30	Granados	10.10.10.232/30	10.10.10.236/30
31	Playas	10.10.10.240/30	10.10.10.244/30
32	Macas	10.10.10.248/30	10.10.10.252/30
33	Tulipanes	10.10.11.32/30	10.10.10.36/30
34	Quito SEPRICARGA	10.10.11.0/30	10.10.11.4/30
35	Guayaquil SEPRICARGA	10.10.11.8/30	10.10.11.12/30
36	Sto.Domingo SEPRICARGA	10.10.11.16/30	10.10.11.20/30
37	Portoviejo SEPRICARGA	10.10.11.24/30	10.10.11.28/30
38	Galapagos	10.10.11.32/30	10.10.11.36/30
39	Matriz Quito Internet	192.168.43.40/30	192.168.34.36/30
40	Gye Internet	192.168.217.196/30	192.168.217.200/30
41	Renazzo	192.168.238.32/30	
42	Holding	192.168.30.89/30	

2.2.2 Direccionamiento en IPv6

Para futuras configuraciones se presenta el direccionamiento en IPv6 de los enlaces de datos a nivel nacional.

Tabla 4. Direccionamiento IPv6 red MPLS

#	Enlace	WAN PRINCIPAL	WAN BACKUP
1	Quito Datos Concentrador	FE80:CAFE:1::/64	FE80:CAFE:2::/64
2	Gye Datos Concentrador	FE80:CAFE:3::/64	FE80:CAFE:4::/64
3	Cuenca	FE80:CAFE:5::/64	FE80:CAFE:6::/64
4	Tena	FE80:CAFE:7::/64	FE80:CAFE:8::/64
5	Manta	FE80:CAFE:9::/64	FE80:CAFE:A::/64
6	Sto. Domingo	FE80:CAFE:B::/64	FE80:CAFE:C::/64
7	Puyo	FE80:CAFE:D::/64	FE80:CAFE:E::/64
8	Tulcán	FE80:CAFE:F::/64	FE80:CAFE:11::/64
9	Loja	FE80:CAFE:12::/64	FE80:CAFE:13::/64
10	Cayambe	FE80:CAFE:14::/64	FE80:CAFE:15::/64
11	Chone	FE80:CAFE:16::/64	FE80:CAFE:17::/64
12	Libertad	FE80:CAFE:18::/64	FE80:CAFE:19::/64
13	Babahoyo	FE80:CAFE:1A::/64	FE80:CAFE:1B::/64
14	Lago Agrio	FE80:CAFE:1C::/64	FE80:CAFE:1D::/64
15	Ambato	FE80:CAFE:1E::/64	FE80:CAFE:1F::/64
16	Guaranda	FE80:CAFE:21::/64	FE80:CAFE:22::/64
17	Riobamba	FE80:CAFE:23::/64	FE80:CAFE:24::/64
18	Ibarra	FE80:CAFE:25::/64	FE80:CAFE:26::/64
19	Esmeraldas	FE80:CAFE:27::/64	FE80:CAFE:28::/64
20	Latacunga	FE80:CAFE:29::/64	FE80:CAFE:2A::/64
21	Portoviejo	FE80:CAFE:2B::/64	FE80:CAFE:2C::/64
22	Quevedo	FE80:CAFE:2D::/64	FE80:CAFE:2E::/64
23	Milagro	FE80:CAFE:2F::/64	FE80:CAFE:31::/64
24	Machala	FE80:CAFE:32::/64	FE80:CAFE:33::/64
25	Coca	FE80:CAFE:34::/64	FE80:CAFE:35::/64
26	Zamora	FE80:CAFE:36::/64	FE80:CAFE:37::/64
27	Naranjal	FE80:CAFE:38::/64	FE80:CAFE:39::/64
28	Bahia	FE80:CAFE:3A::/64	FE80:CAFE:3B::/64
29	Azogues	FE80:CAFE:3C::/64	FE80:CAFE:3D::/64
30	Granados	FE80:CAFE:3E::/64	FE80:CAFE:3F::/64
31	Playas	FE80:CAFE:41::/64	FE80:CAFE:42::/64
32	Macas	FE80:CAFE:43::/64	FE80:CAFE:44::/64

33	Tulipanes	FE80:CAFE:45::/64	FE80:CAFE:46::/64
34	Quito SEPRICARGA	FE80:CAFE:47::/64	FE80:CAFE:48::/64
35	Guayaquil SEPRICARGA	FE80:CAFE:49::/64	FE80:CAFE:4A::/64
36	Sto.Domingo SEPRICARGA	FE80:CAFE:4B::/64	FE80:CAFE:4C::/64
37	Portoviejo SEPRICARGA	FE80:CAFE:4D::/64	FE80:CAFE:4E::/64
38	Galapagos	FE80:CAFE:4F::/64	FE80:CAFE:51::/64

En la subred que tiene 128 bits los 64 bits son designados para la red y los restantes 64 bits son para los host, cada host será construido dependiendo la dirección MAC de la tarjeta.

2.2.3 Enrutamiento

En la nueva topología de la red MPLS el enrutamiento se realizará mediante el protocolo de enrutamiento dinámico BGP, las métricas que serán utilizadas son: local-preference para las subredes de entrada desde el PE hacia el CE, y as-path para las subredes de salida desde el CE hacia el PE.

El mayor valor de la métrica local-preference será designado como la mejor ruta de entrada y el menor valor de la métrica as-path será designado como la mejor ruta de salida, con estas dos métricas se podrá designar el enlace principal y el de backup en cada uno de los puntos.

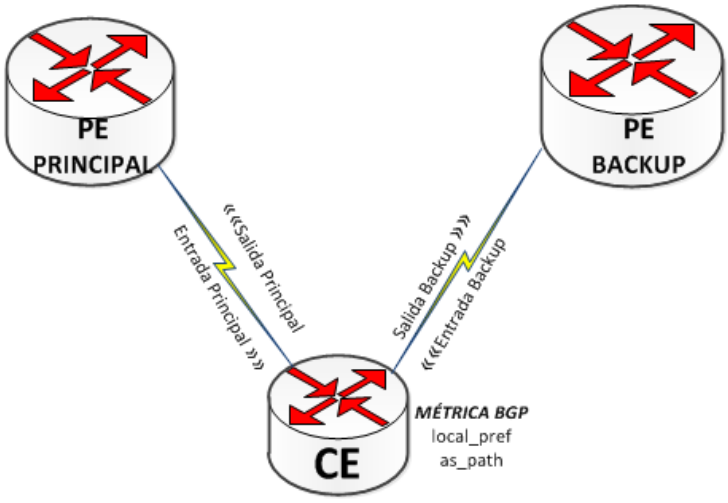

Figura 19. Enlace WAN entre CE y dos PE con BGP

En determinadas ciudades solo existe un PE y no se puede emplear dual PE, por ende, el enlace principal y backup se configura en el mismo PE, en estos casos aparte de la métrica local-preference y as-path, se utilizará la métrica weight para definir correctamente la prioridad de cada enlace.

En la figura No. 20, se verifica que las métricas de local_pref y as-path son configuradas en los vecinos del CE tanto del principal como del backup y el wight es configurado de la misma forma en los vecinos del PE.

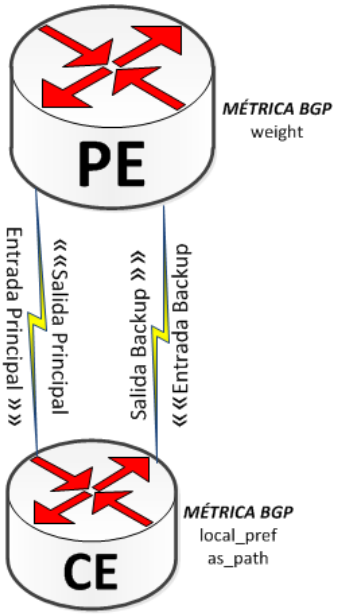

Figura 20. Entre WAN entre CE y un PE

En los router virtuales de datos de matriz, se implementará una ruta por defecto con el próximo salto (next hop) al router virtual de acceso a internet, esta ruta será difundida en los routers PE en la red MPLS, brindando acceso al internet a las sucursales a nivel nacional, como primer opción de acceso al internet será matriz Quito y la segunda matriz Guayaquil.

En todas las sucursales también se configurará BGP como protocolo de enrutamiento en la WAN, es decir, la configuración entre el CE y PE. Sin embargo, en ciertas ciudades no puede pasar la vlan directamente debido que la última milla no es provista por Puntonet, en estos casos se procederá a realizar un túnel GRE entre el CE y el PE para integrar a la red MPLS.

En la figura No. 21, se encuentra el diagrama en la cual no se tiene con la infraestructura provista por Puntonet y se emplea Tunnel GRE, para tener comunicación en la red MPLS.

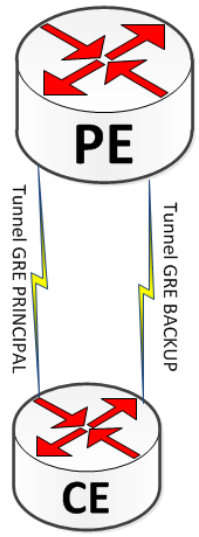

Figura 21. Enlace WAN entre CE y PE con túnel GRE

Los enlaces de acceso al internet también se configurarán con BGP y tendrán una subred pública mascará 30, se empleará un sistema autónomo AS diferente al de datos, acceso a internet y datos se levantará EBGP entre el PE y CE por trabajar en diferentes sistemas autónomos.

Cabe mencionar que todas estas métricas utilizan diferentes argumentos o parámetros de la red para su funcionamiento, por lo que no se podría realizar una comparación de distancia administrativa entre las misma.

2.2.4 Equipos

Los equipos que se implementará en matriz Quito es un router cisco 2921, router Mikrotik 2011 y ONT Calix, el router cisco 2921 tiene tres interfaces GigaEthernet incorporadas y cuatro ranuras EHWIC una de las cuales se instalará una tarjeta HWIC-4ASEW, en total se tendrá 7 puertos disponibles, la interfaz GigaEthernet0 será para el enlace principal de internet, GigaEthernet1 designada para principal de datos, la interfaz GigaEthernet2 se recogerá los enlaces de backup de datos y acceso al internet y las 4 interfaces de la tarjeta HWIC se asignará para LAN de datos y la pública de internet. El router Mikrotik

2011 en la interfaz ether1 la IP pública y del 3 al 10 para la LAN de internet. El ONT calix tiene 4 puertos para configurar vlan independientes, es decir, se puede dar un servicio por cada puerto.

Las sucursales utilizarán routers de tres interfaces las cuales pueden ser de capa 3 o de capa 2, en la mayoría de las sucursales se utilizarán los mismos equipos que se encuentran funcionando en la red Ethernet, los routers son de marca Cisco o Mikrotik.

En todos los enlaces se procederá a verificar el cableado perteneciente al proveedor, que es desde la última milla hasta el CE y si es necesario se cambiará a categoría UTP 6 para garantizar los servicios prestados.

2.2.5 Esquema de la red nacional

Todos los enlaces que tienen servicio de datos se configurará dentro de una VRF en los PEs, esta VRF es exclusiva para la empresa Urbano Express, proporcionando seguridad y aislando la red privada de la empresa, es decir una VPN en MPLS, de esta manera todas las sucursales y matrices que están en esta VRF podrán tener comunicación de extremo a extremo mediante la red de transporte MPLS del proveedor de servicios de internet Puntonet.

Todos los enlaces tienen que verificar el momento de la migración que tenga conectividad con el PE que crea las vecindades BGP, y difundas las rutas del CE al PE, con esta tendrá conectividad con el resto puntos a nivel nacional.

En la figura 22 se detalla como estarán conectados los CE a cada uno de los PEs de la red MPLS y la interconexión entre PEs.

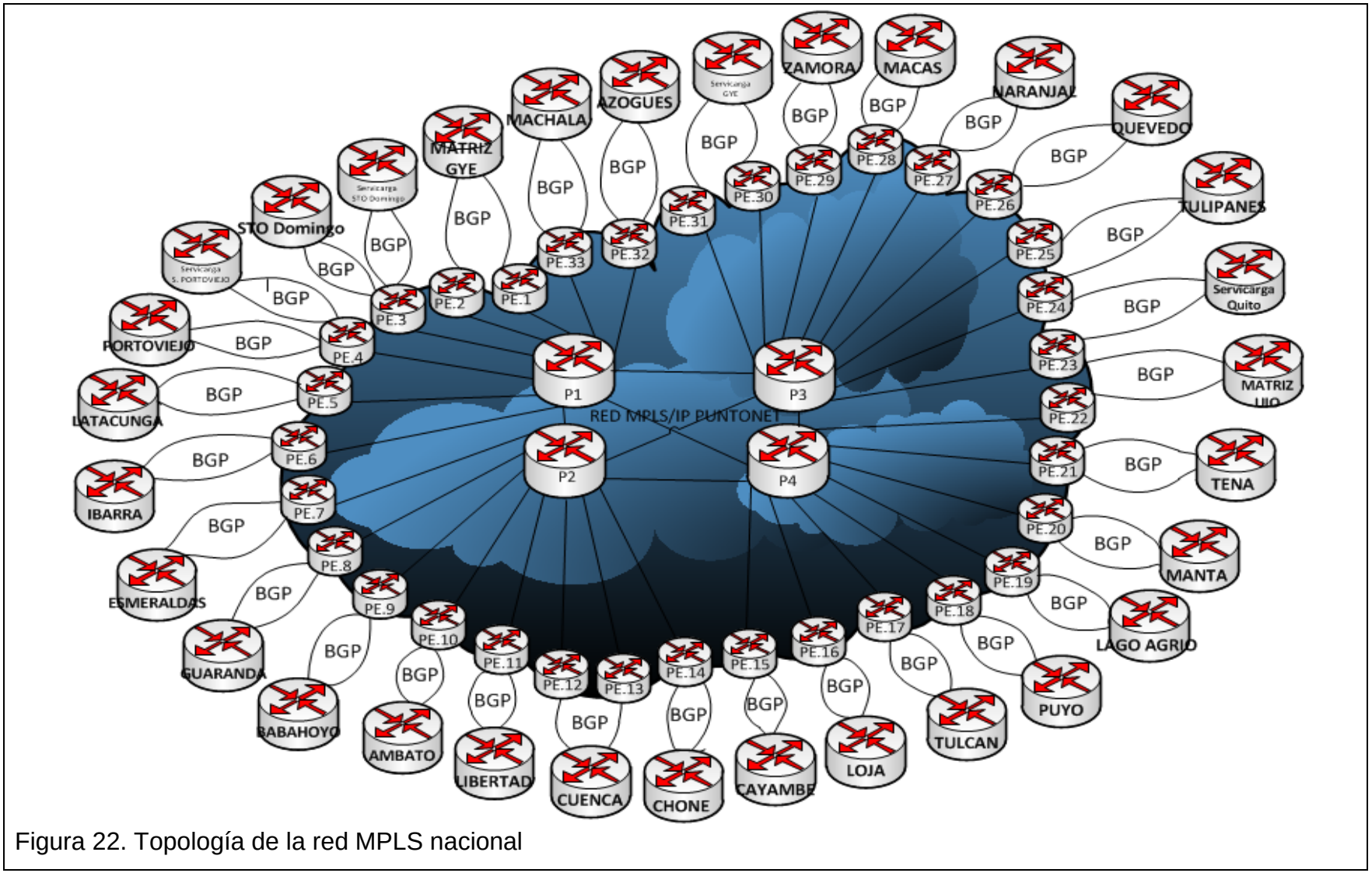

Figura 22. Topología de la red MPLS nacional

3. Capítulo III. Implementación de la Nueva Tecnología

3.1 Instalación de concentradores

Las matrices ubicadas en las ciudades de Quito y Guayaquil tendrán directamente acceso a internet y todas las sucursales a nivel nacional se conectarán a matriz Quito como primera opción para salida a internet, en el caso que exista un problema en el concentrador de internet de Quito, como segunda opción se enrutará de manera automática el tráfico de internet mediante el protocolo BGP hacia el concentrador de internet Guayaquil.

Los enlaces de datos no se implementará el modelo de concentrador debido que las sucursales se pueden interconectar entre si directamente mediante la red MPLS, es decir, si la sucursal Puyo desea comunicarse con la del Tena no necesita realizar peticiones a matriz Quito o Guayaquil.

3.1.1 Concentrador Quito

La matriz principal se encuentra en la ciudad de Quito, la cual se instaló un router cisco para brindar los servicios de datos y acceso a internet para las sucursales, el cisco 2900 tiene tres interfaces de capa 3, GigabitEthernet0/1, GigabitEthernet0/2 y GigabitEthernet0/3, también una interfaz HWIC FastEthernet0/0/0 a la FasEthernet0/0/3.

La versión del router cisco es "flash0:c2900-universalk9-mz.SPA.154-1.T1.bin", con una memoria de 1363648564 bps.

Este enlace tiene redundancia a nivel de la última milla con fibra óptica los dos enlaces tanto principal como backup, en la figura No. 23 se verifica la topología del concentrador de matriz en la ciudad de Quito.

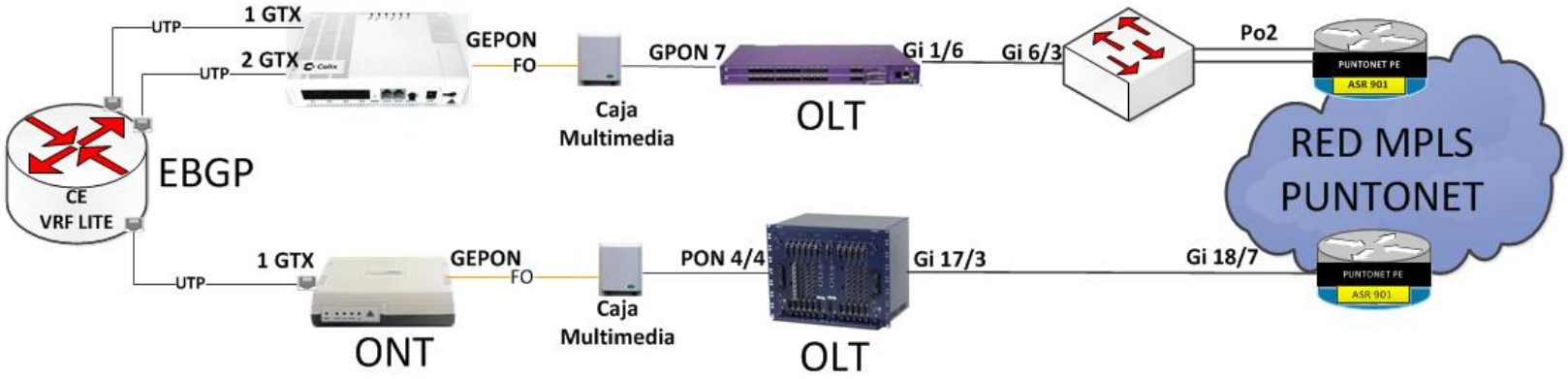

Figura 23.- Topología de red MPLS Matriz Quito

a) En la figura 23 se indica la topología hasta la WAN del cliente, la LAN es administrada directamente por el cliente.

3.1.1.1 ENLACE PRINCIPAL

A continuación se detalla las configuraciones que se realizó en cada uno de los equipos PE, SW de core, OLT, ONT y el CE, en primera instancia se empleó 4 vlan, dos subredes de 4 IPs privadas para la red de datos MPLS, dos subredes de 4 IPs privadas para enlace de acceso a internet y una subred pública para acceso a internet. Primero se levantó los enlace principales de datos y acceso a internet de la siguiente manera:

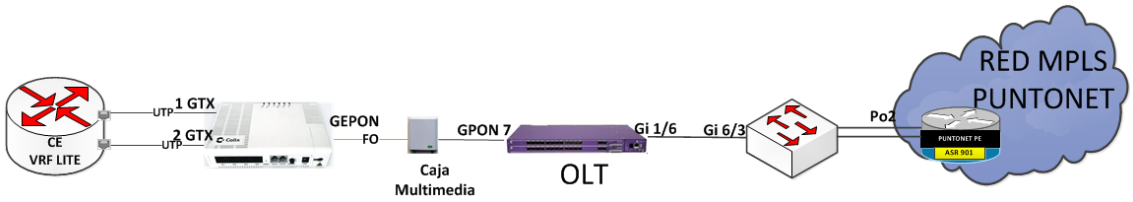

Figura 24. Enlace principal Datos e Internet Quito

- **En el PE principal**

Se creó la VRF con el nombre de dat1010 única para la empresa Urbano Express en la red MPLS de Puntonet para los enlaces de datos.

PE02(config-vrf)#ip vrf dat1010

Se configuró el router distinguer en relación con el sistema autónomo de BGP y la VRF.

PE02(config-vrf)#rd 56001:1010

Importar y exportar los prefijos de la red e importa la vrf de monitoreo para alcanzar desde la intranet de Puntonet.

PE02(config-vrf)#route-target both 56001:1010

PE02(config-vrf)#route-target import 56001:888

Con el comando show run vrf dat1010 se evidenció que las configuraciones realizadas están correctas.

ip vrf dat1010

rd 56001:1010

route-target export 56001:1010

route-target import 56001:1010

route-target import 56001:888

El enlace de internet también se configuró en la red MPLS en la VRF internet que permite el acceso a internet, por tal motivo no se creó una VRF para los enlaces a internet.

Una vez creada y activada la VRF se procedió activar la interfaz VLAN correspondiente al enlace, en este caso en la VLAN 2105 con su respectiva descripción, la VRF y la IP correspondiente.

PE02(config)#interface vlan 2105
PE02(config-if)#description
URBANO_EXPRESS_MATRIZ_DATOS_MPLS_PRINCIPAL
PE02(config-if)#ip vrf forwarding dat1010
PE02(config-if)#ip address 10.10.10.1 255.255.255.252
PE02(config-if)#no shutdown

La VLAN designada para el enlace de internet para las sucursales es la número 50

PE02(config)#interface vlan 50
PE02(config-if)#description URBANO_EXPRESS_MATRIZ_INTERN_PRINCIPAL
PE02(config-if)#ip vrf forwarding internet
PE02(config-if)#ip address 192.168.43.41 255.255.255.252
PE02(config-if)#no shutdown

Una vez creadas las interface VLAN se procedió activar y pasar las vlan en el PE en la interface Port-channel2 con la que se conecta con el SW del Core, esta mediante un service instance.

PE02(config)#interface Port-channel10
PE02(config-if)#service instance 2105ethernet
PE02(config-if-srv)#description
URBANO_EXPRESS_MATRIZ_DATOS_MPLS_PRINCIPAL
PE02(config-if-srv)#encapsulation dot1q 2105
PE02(config-if-srv)#rewrite ingress tag pop 1 symmetric

PE02(config-if-srv)#bridge-domain 2105

PE02(config)#interface Port-channel10
PE02(config-if)#service instance 50 ethernet
PE02(config-if-srv)#description
URBANO_EXPRESS_MATRIZ_INTERNET_PRINCIPAL
PE02(config-if-srv)#encapsulation dot1q 50
PE02(config-if-srv)#rewrite ingress tag pop 1 symmetric
PE02(config-if-srv)#bridge-domain 50

Se verifica que las vlans se encuentre activada correctamente con el siguiente comando.

PE02#show vlan id 2105
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
2105 VLAN2105 active
PE02#show vlan id 50
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
50 VLAN50 active

- **En el switch de core**

Se activó y pasó las vlans por los puertos específicos de la conexión, generalmente los puertos en switch de core las vlans se encuentran pasadas en rangos en modo trunk, por tal motivo, el momento que se active la vlan se verifica la misma pasada por diferentes puertos del switch causando lasos en la red y consumo de los recursos (memoria, cpu) de los equipo switch, para eliminar estos posibles inconvenientes se remueve la vlan de los puertos en los que no tendría que estar pasados.

Para verificar los puertos en los cuales se encuentra pasada las vlan se realiza con el siguiente comando: show vlan id (número de la vlan)

SW-CORE-L3#show vlan id 2105

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

2105 VLAN2105 active Po2, Gi1/2, Gi1/5, Gi1/8, Gi1/9
Gi1/39, Gi1/42, Gi1/47, Gi1/48
Gi5/28, Gi5/29, Gi5/30, Gi6/3

Como se puede verificar en el resultado del comando show vlan id 2105 esta vlan se encuentra pasada por varios puertos que no tendría que estar, por tal motivo se procede a eliminar la vlan de los puertos erróneos, en este caso solo tiene que estar pasado en las intercaces port-channel 2 y GigabitEthernet 6/3.

Como buena práctica se recomienda antes de eliminar la vlan de la interfaz verificar las vlans que se encuentren pasadas en ese momento por la interfaz, esto debido que, si existe un error como borrar el resto de vlans pasadas en la interfaz puede volver a configurarles.

Verificó las vlan que se encuentres pasadas en la interfaz.

SW-CORE-L3#show run in GigabitEthernet 1/2
Building configuration...
Current configuration : 213 bytes
!
interface GigabitEthernet1/2
*description *** LINK TO SW-MONJAS Gi0/51 BACKHAUL FO PRINCIPAL ****
switchport trunk allowed vlan 1-1034,1036-1593,1595-2624,2626-4094
switchport mode trunk
load-interval 30
end

Se ingresó a la interfaz para remover la vlan.

SW-CORE-L3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CORE-L3 (config)# interface GigabitEthernet1/2

SW-CORE-L3 (config-if)#switchport trunk allowed vlan remove 2105
SW-CORE-L3 (config-if)#switchport trunk allowed vlan remove 50

Por último, pero no menos importante, se verificó en la interfaz que la única vlan removida sea la 2105 y 50.

SW-CORE-L3#show run in GigabitEthernet 1/2
Building configuration...
Current configuration : 213 bytes
!
interface GigabitEthernet1/2
*description *** LINK TO SW-MONJAS Gi0/51 BACKHAUL FO PRINCIPAL ****
switchport trunk allowed vlan 1-49,51-1034,1036-1593,1595-2104,2106-2624,2626-4094
switchport mode trunk
load-interval 30
end

Este mismo proceso se realizó en cada uno de la interfaces Gi1/3, Gi1/5, Gi1/8, Gi1/9, Gi1/39, Gi1/42, Gi1/47, Gi1/48, Gi5/28, Gi5/29, Gi5/30, en las cuales se encontraba pasada las vlans de forma inadecuada, de esta manera se tiene activada y pasada en los dos únicas interfaces como se puede evidenciar.

SW-CORE-L3#show vlan id 2105

VLAN	*Name*	*Status*	*Ports*
2105	*VLAN2105*	*active*	*Po2, Gi6/3*

SW-CORE-L3#show vlan id 50

VLAN	*Name*	*Status*	*Ports*
50	*VLAN50*	*active*	*Po2, Gi6/3*

- **En la línea de terminal óptica OLT Calix**

De similar forma se activó y pasó la vlan en los puerto de UPLINK que se conecta con el SW de core y en el puerto GPON que se conecta a la red óptica hasta

llegar al ONT. La configuración en un OLT y ONT de marca Calix se realizó de la siguiente manera.

Un vez conectado el ONT CALIX, en el lapso de un minuto se engancha, físicamente se detecta que se enciende el led OPTICA POWER de color verde fijo, verificamos en el item **ONTs** en la pestaña **DISCOVERED ONTs** la FSAN SERIAL del ONT, selecciona la FSAN posteriormente escogemos en la pestaña **ACTION** en la opción **Link to new Provisioning.**

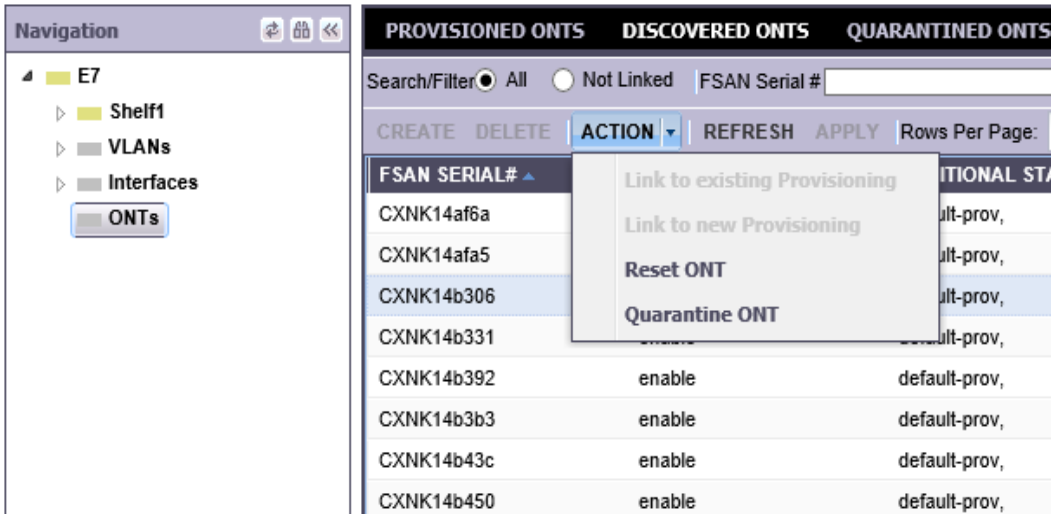

Figura 25. Descubrir un ONT Calix

Mostrará una nueva ventana en el item **ONT PROFILE** selecciona el modelo del ONT en esta caso se usa el **T072G** y aceptamos el cambios **OK**.

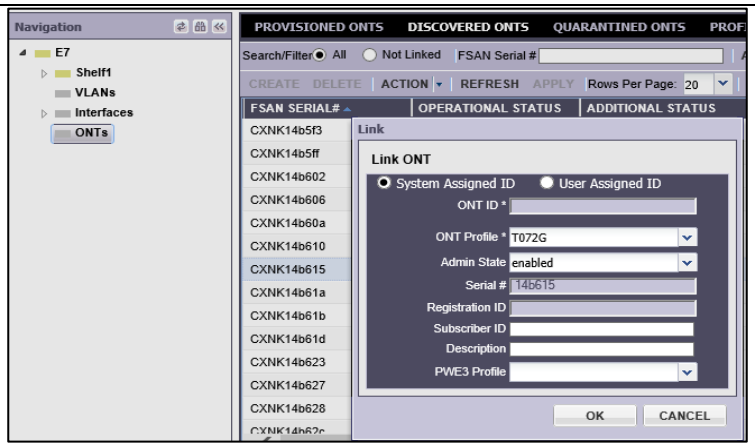

Figura 26. Provisionar de un ONT Calix

Verificar ONT provisionado

En el item **ONTs** la pestaña **PROVISIONED ONTS** == **PROVIONING** se verificó el número de ONT asignado a la FSAN. Ejemplo **ONT48** pertenece a la FSAN **14b306**, con esto evidenciamos que ya se encuentra pro visionado el ONT correctamente.

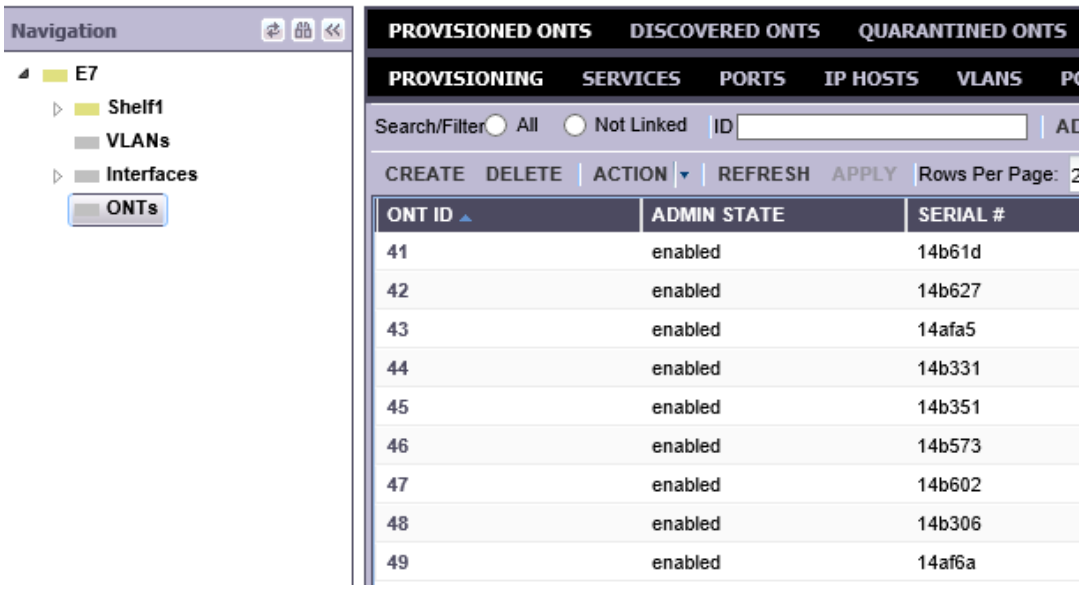

Figura 27. Designación del número de ONT

Crear la vlan en el OLT Calix

En el item **VLANs**, la pestaña **PROVISIONING**, selecciona la pestaña **CREATE**, en la nueva ventana que presenta ingresamos en **ID** = Número de vlan a crear, **Name** = vlan_(Número de vlan) y activamos el **DHCP Snoop** = Activar posteriormente guardamos los cambios.

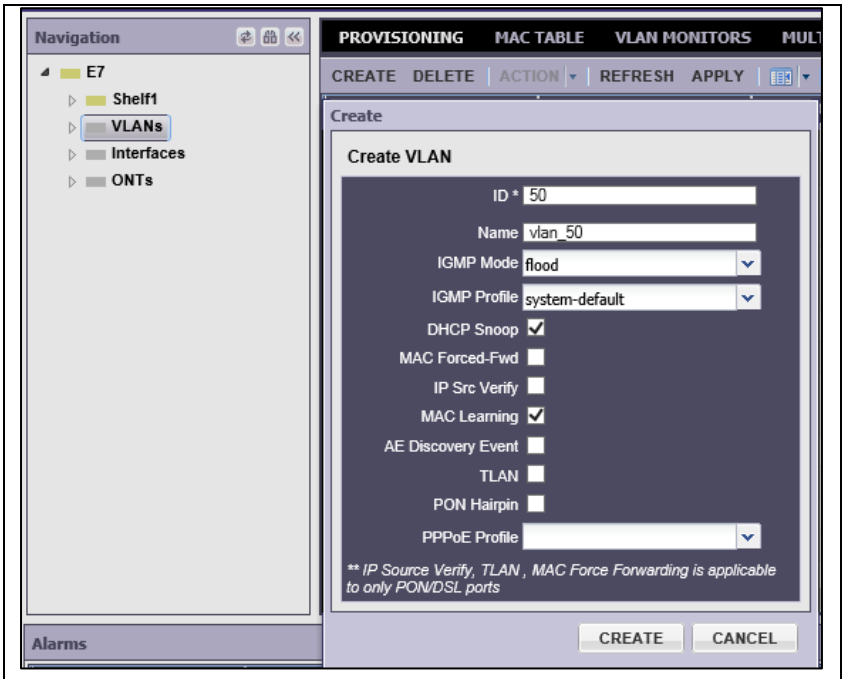

Figura 28. Creación de vlan en OLT Calix

Una vez realizado el anterior paso se verifica en **VLANs --- PROVIONING** la vlan creada, seleccionamos la vlan con un doble clip para taggear en el puerto de uplink.

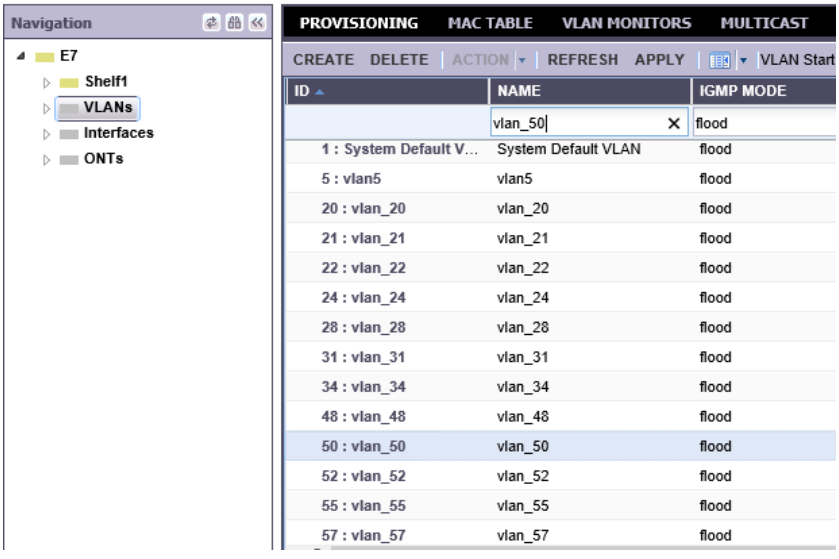

Figura 29. Listado de vlan en el OLT Calix

Taggear la vlan en el puerto uplink

En el item **VLANs** en la pestaña **PROVISIONING** --- **ACTION** seleccionamos la opción **Add/Remove VLAN Members.**

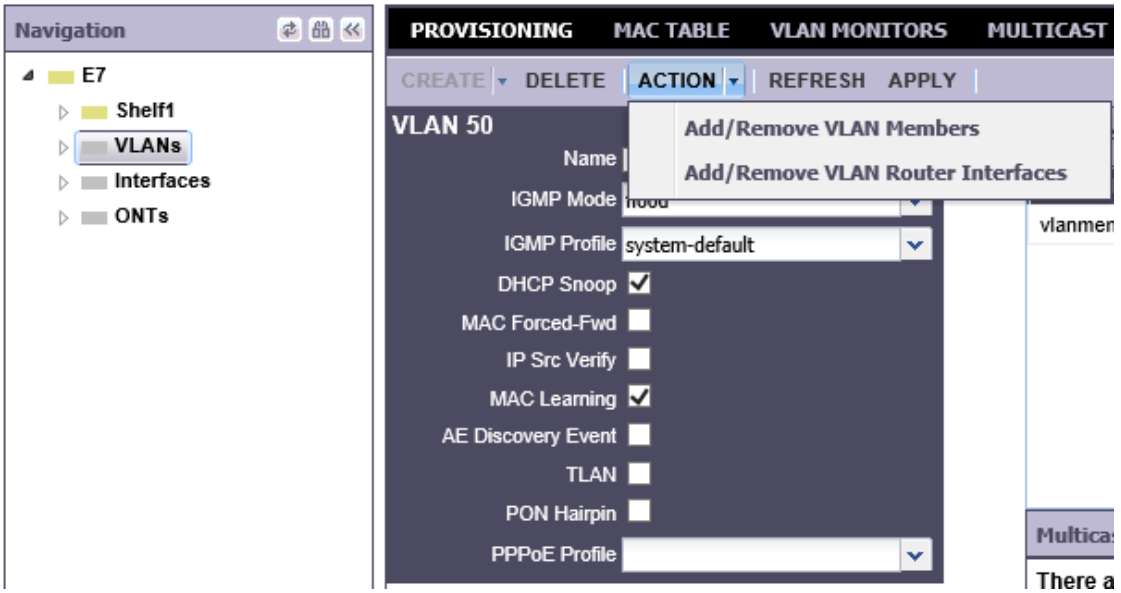

Figura 30. Taggerar la vlan en el puerto de UPLINK

En la presente venta seleccionamos el puerto UPLINK en el cual se taggera la vlan ejemplo la vlan 50 se taggea en el puerto ETHINTF: 6/3, con las fechas (> o <) **Add /Remove** el puerto seleccionado.

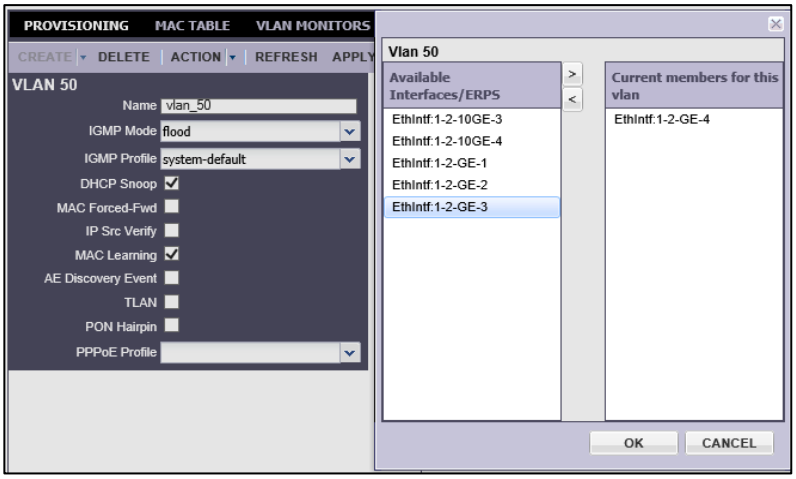

Figura 31. Taggerar la vlan en el puerto de UPLINK

Crear un perfil de ancho de banda

En el item **E7** la pestaña **PROFILES --- SERVICE --- ETHERNET BANDWIDTH --- PROFILES** selecciona **CREATE** se despliega una nueva ventana para ingresar los siguientes datos, **Name** = bw_(valor de AB), **Peak Rate for upstream** = (valor de AB UP)Kpbs, **Peak Rate for Downstream** = (valor de AB Down)Kbps, una vez ingresados los valores se crear el perfil de AB **CREATE**, el mismo perfil de AB puede ser utilizado por varios clientes.

Nota: El resto de valores van por defecto no se cambia.

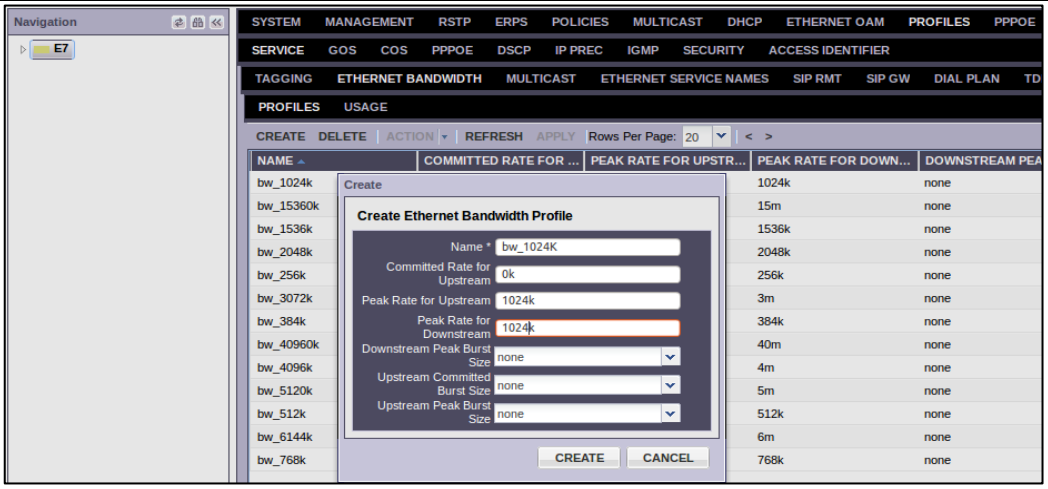

Figura 32. Perfil de ancho de banda en OLT Calix

Crear un tagging

En el item **E7** la pestaña **PROFILES --- SERVICE --- TAGGING – TAG ACTIONS – PROFILES** seleccionamos **CREATE** se ingresa los siguientes valores **Name** = Nombre del tag, **Action** = add tag, **Match list** = 1 – (all-untagged), **S-VLAN (outer Tag)** = Specified in Service(la vlan se especifica el momento que se crea el servicio.)

Nota: El resto de valores van por defecto.

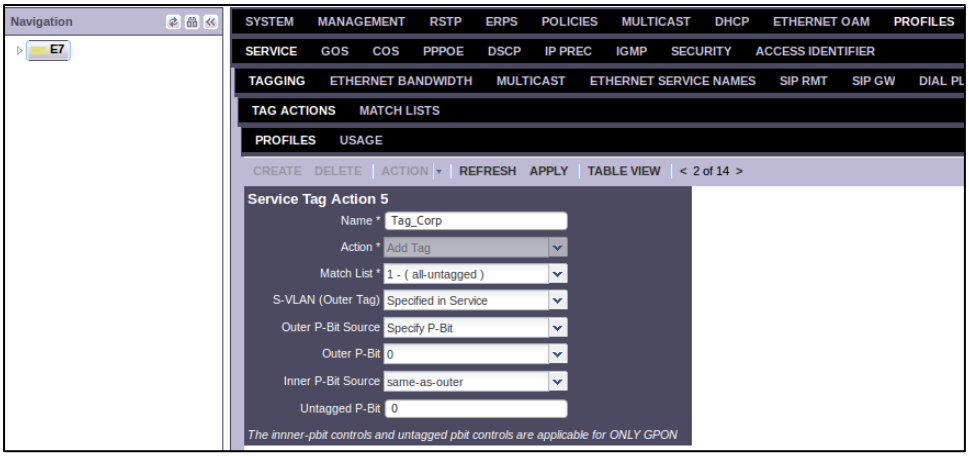

Figura 33. Perfil de tagging en un OLT Calix

Asignación de recursos en el ONT

Se busca el ONT al cual se asignara los servicios dependiendo del puerto GPON al que se encuentra, en cada ONT se tiene los puertos GE1, GE2, GE3 y GE4, una vez seleccionado el ONT ejemplo el ONT48, en la pestaña **SERVICES --- TABLE --- CREATE** escogemos la opción **Data Service**

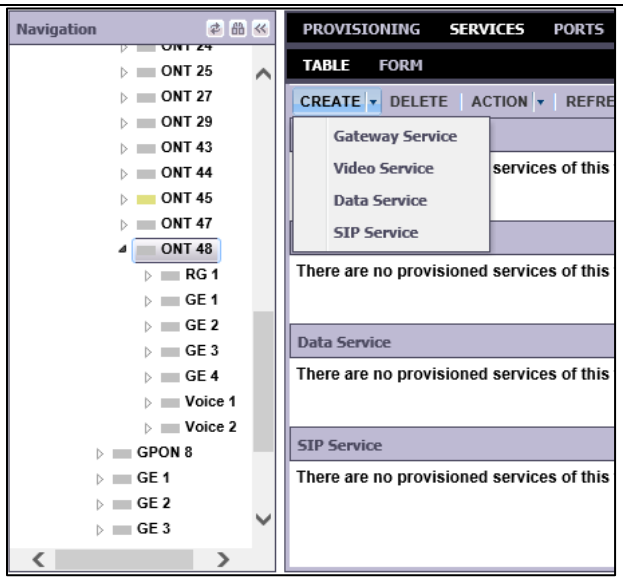

Figura 34. Selección del servicio en el ONT Calix.

En la nueva ventana ingresamos los siguientes datos: **Subscriber Port** = El ONT tiene 4 port GigaEtherne (selecciono uno para cada servicio, si tiene datos o internet cada servicio va en diferente puerto), **Subscriber ID** = Codigo_Plan del netpus, Description = Nombre de la empresa en mayúsculas, **Service Name** = Data 1, **BW Profile** = Seleccionamos el AB de la lista que se creó anteriormente, **Service Tag Action** = Seleccionamos el Tag creado para cada vlan, **S-VLAN(Outer Tag)** = Número de VLAN presionamos **CREATE.**

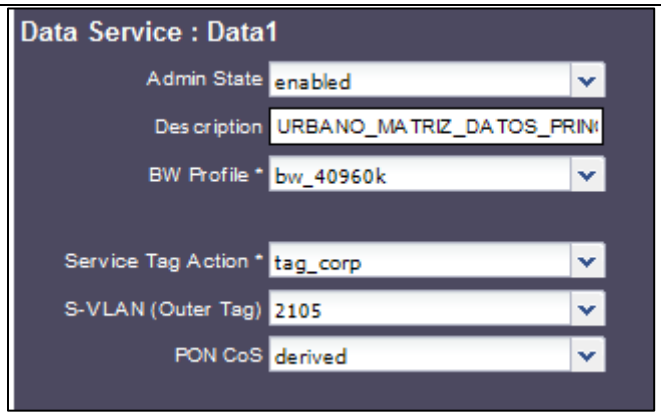

Figura 35. Recursos para el enlace de Datos Principal

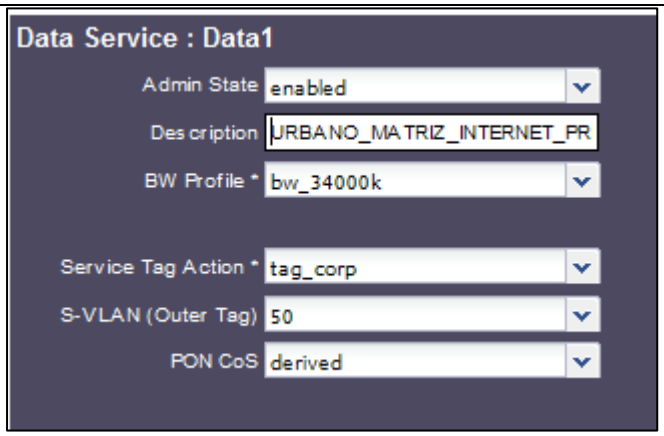

Figura 36. Recursos para el enlace de Internet Principal

Los servicios creados en el ONT se encuentran en **ONT --- SERVICES --- TABLE** en el cual se confirma los datos como Puerto del ONT asignado, código_plan, nombre de la empresa, ancho de banda y vlan.

- **Router de border del cliente CE**

En el CE se procedió a virtualizar para brindar los servicios de datos y acceso a internet, pero antes se implementó las configuraciones básicas y los accesos al router para administración y seguridad del equipo.

Se ingresó un nombre al router.

routers(config)#hostname URBANO_EXPRESS_DATOS_INTERNET_MATRIZ
URBANO_EXPRESS_DATOS(config)#exit
URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#

Se desactivó la búsqueda recurrente de dominios erróneos, evitando que el router se cuelgue temporalmente si se ingresa un comando erróneo.

URBANO_EXPRESS_DATOS(config)#no ip domain lookup

Una contraseña de seguridad al momento de ingresar al mode de configuración global del router.

URBANO_EXPRESS_DATOS(config)#enable secret wwwww

Seguridad al momento de ingresar por consola al cisco.

URBANO_EXPRESS_DATOS(config)#line console 0
URBANO_EXPRESS_DATOS(config-line)#password wwwww
URBANO_EXPRESS_DATOS(config-line)#login

Un usuario local para la administración del router una vez activado el telnet, este usuario tiene privilegio 15 al cual no va pedir la contraseña para ingresar al modo de configuración global.

URBANO_EXPR*ESS_DATOS(config)#username uwwwww privilege 15 password pwwwww*

Se configuró el acceso al router mediante telnet con el usuario local.

URBANO_EXPRESS_DATOS(config)#line vty 0 4
URBANO_EXPRESS_DATOS(config-line)#login local
URBANO_EXPRESS_DATOS(config-line)#transport input all

Se procedió a encriptar las contraseñas del router por seguridad,
URBANO_EXPRESS_DATOS(config)#service password-encryption

Un mensaje de alerta si alguien quiere ingresar al router o para verificar a quien le pertenece el router.
URBANO_EXPRESS_DATOS(config)#banner motd #

PUNTONET S.A.
Acceso restringido!!!
Solo personal autorizado - FC.

Fecha: 2015_09_14 E-mail: cccorporativo@puntonet.ec
Empresa: URBANO_EXPRESS_MATRIZ_DATOS_INTERNET

#
Una vez que se implementó las configuraciones básicas del router, creó una VRF en el CE con el nombre de datos para el servicio de datos y otra VRF internet.
URBANO_EXPRESS_DATOS(config)#ip vrf datos
URBANO_EXPRESS_DATOS(config-vrf)#rd 2:2
URBANO_EXPRESS_DATOS(config-vrf)#route-target import 2:2

URBANO_EXPRESS_DATOS(config)#ip vrf internet
URBANO_EXPRESS_DATOS(config-vrf)#rd 1:1
URBANO_EXPRESS_DATOS(config-vrf)#route-target import 1:1

En la interface GigabitEthernet0/0 que fue designada para el enlace de datos se configuró la IP del enlace principal.

URBANO_EXPRESS_DATOS(config)#interface GigabitEthernet0/0
URBANO_EXPRESS_DATOS(config-if)#ip vrf forwarding datos
URBANO_EXPRESS_DATOS(config-if)#ip address 10.10.10.2 255.255.255.252
URBANO_EXPRESS_DATOS(config-if)#no shutdown

En la interface GigabitEthernet0/1 que fue designada para el enlace de internet se configuró la IP del enlace principal.

URBANO_EXPRESS_DATOS(config)#interface GigabitEthernet0/1
URBANO_EXPRESS_DATOS(config-if)#ip vrf forwarding internet
URBANO_EXPRESS_DATOS(config-if)#ip addre 192.168.43.42 255.255.255.252
URBANO_EXPRESS_DATOS(config-if)#no shutdown

Con estas configuraciones se obtuvo conectividad desde el PE hacia el CE y viceversa.

PE hacia el CE

PE02#ping vrf dat1010 10.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

PE02#ping vrf internet 192.168.43.42
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.43.42, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CE hacia el PE

URBANO_EXPRESS_DATOS#ping vrf datos 10.10.10.1
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

URBANO_EXPRESS_DATOS#ping vrf internet 192.168.43.41

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.43.41, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

3.1.1.2 ENLACES DE BACKUP

Una vez que se tuvo conexión exitosa con el enlace de datos e internet principal se procedió a configurar el enlace de backup que tiene como última milla fibra óptica con ruta alterna con marca corecess, para este enlace también se empleó una VLANs para datos y otra para acceso a internet, estos enlaces se configuró en otro PE el cual tiene conexión directa con el OLT de marca corecess con esto garantizamos una redundancia a nivel de PE, OLT y SW de core debido que los enlaces principales están aislados de los enlaces de backup.

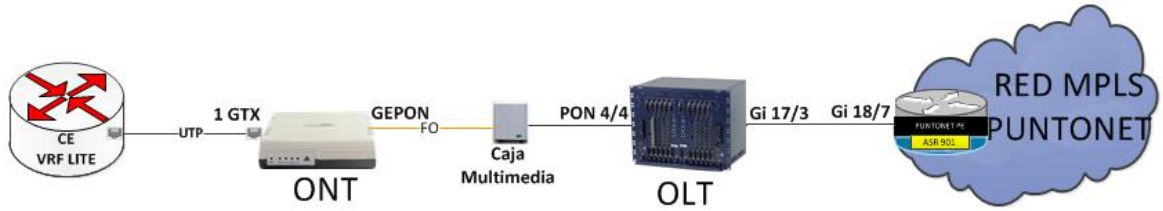

Figura 37. Enlace principal Datos e Internet

- **Enlace de backup datos e internet en el PE**

En el PE de backup de la red MPLS de Puntonet se procedió a configurar la VRF dat1010 designada anteriormente para la empresa Urbano Express.

PE03(config-vrf)#ip vrf dat1010

Se configuró el router distinguer en relación con el sistema autónomo de BGP y la VRF.

PE03(config-vrf)#rd 56001:1010

Importar y exportar los prefijos de la red.

PE03(config-vrf)#route-target both 56001:1010

PE03(config-vrf)#route-target both 56001:888

Con el comando show running vrf dat1010 se evidenció que las configuraciones realizadas están correctas.

ip vrf dat1010

rd 56001:1010

route-target export 56001:1010

route-target import 56001:1010

route-target import 56001:888

Con la importación de los prefijos de la VRF monitoreo 888 permite tener acceso a las subredes de MPLS de la empresa Urbano Express desde la intranet de Puntonet.

El enlace de internet de backup se activó en la red MPLS en la VRF internet que permite el acceso a internet, esta vrf ya se encuentra activada en el PE de backup.

Una vez creada y activada la VRF se procedió activar la interfaz VLAN correspondiente al enlace de datos backup, en este caso en la VLAN con su respectiva descripción, la VRF y la IP correspondiente.

PE03(config)#interface vlan 3216

PE03(config-if)#description URBANO_EXPRESS_MATRIZ_DATOS_MPLS_BK

PE03(config-if)#ip vrf forwarding dat1010

PE03(config-if)#ip address 10.10.10.5 255.255.255.252

PE03(config-if)#no shutdown

La VLAN designada para el enlace de internet bk para las sucursales es la 3222

PE03(config)#interface vlan 3222

PE03(config-if)#description URBANO_EXPRESS_MATRIZ_INTERN_BK

PE03(config-if)#ip vrf forwarding internet

PE03(config-if)#ip address 192.168.43.37 255.255.255.252
PE03(config-if)#no shutdown

Una vez creadas las interface VLAN se procedió activar y pasar las vlan en el PE en la interface GigabitEthernet18/7 con la que se conecta al OLT de marca corecess, esta mediante un service instance.

PE03(config)#interface GigabitEthernet18/7
PE03(config-if)#service instance 3216 ethernet
PE03(config-if-srv)#description
URBANO_EXPRESS_MATRIZ_DATOS_MPLS_BK
PE03(config-if-srv)#encapsulation dot1q 3216
PE03(config-if-srv)#rewrite ingress tag pop 1 symmetric
PE03(config-if-srv)#bridge-domain 3216
PE03(config)#interface GigabitEthernet18/7
PE03(config-if)#service instance 3222 ethernet
PE03(config-if-srv)#description URBANO_EXPRESS_MATRIZ_INTERNET_BK
PE03(config-if-srv)#encapsulation dot1q 3222
PE03(config-if-srv)#rewrite ingress tag pop 1 symmetric
PE03(config-if-srv)#bridge-domain 3222

Se verifica que las vlans se encuentren activadas correctamente con el siguiente comando.

PE03#show vlan id 3216

VLAN	*Name*	*Status*	*Ports*
3216	*VLAN3216*	*active*	

PE03#show vlan id 3222

VLAN	*Name*	*Status*	*Ports*
3222	*VLAN3222*	*active*	

- **OLT Óptica Line Terminal Corecess**

En el OLT de marca Corecess en el cual se configuró los enlaces de backup, las configuraciones se realizaron mediante comandos por consola ingresando al OLT.

El ONT se identificó con su única MAC ADDRESS, en relación con esta MAC se generó las configuraciones para el puerto 2 del ONT en el cual se configuró a modo trunk para pasar las VLAN de datos y acceso a internet por el mismo puerto, por consiguiente, las VLANs fueron destagueadas en el CE.
Por el puerto solo se configuró a modo trunk y el ancho de banda para los dos enlaces de datos e internet, la restricción de ancho de banda para cada servicio se realizó en el CE, en la configuración del ancho de banda se consideró la velocidad de subida y de bajada, en este caso se tiene 70 Mbps simétricos con un nivel de compartición de 1 a 1, es decir, un canal dedicado. OLT-UIO-GEPON(config)# port epon 4/4 link-mac 0090a306a7c2 down-bw 71680 71680 3 delay tolerant
% 1/1 00:90:a3:06:a7:c2 Set bandwidth. Done
OLT-UIO-GEPON(config)# port epon 4/4 link-mac 0090a306a7c2 up-bw 71680 71680 3 delay tolerant
% 1/1 00:90:a3:06:a7:c2 Set bandwidth. Done

Con el commando show running y filtrando los últimos cuatro dígitos de la Mac Address del ONT se evidenció que las configuraciones estén correctas.
OLT-UIO-GEPON# sh run port epon 4/4 | include a7c2
port epon 4/4 link-mac 0090a306a7c2 up-bw 71680 71680 3 delay tolerant
port epon 4/4 link-mac 0090a306a7c2 down-bw 71680 71680 3 delay tolerant
De similar forma que en todos los equipos se tagueo las VLANs en los puertos de uplink al PE de backup y la red óptica en el puerto EPON 4/4.

Puerto GEPON vlan datos e internet.
OLT-UIO-GEPON(config)# dot1q port epon 4/4 tag 3216
OLT-UIO-GEPON(config)# dot1q port epon 4/4 tag 3222

Puerto de UPLINK vlan datos e internet

OLT-UIO-GEPON(config)# dot1q port gigabitethernet 17/3 tag 3216
OLT-UIO-GEPON(config)# dot1q port gigabitethernet 17/3 tag 3222

Las configuraciones realizadas a las vlans se evidencia con el comando show vlan filtrando la vlan que se tiene configurado, en la cual se verificó que las dos vlans se encuentran pasadas correctamente.

OLT-UIO-GEPON# show vlan | include 3216

4/4 tagged:1089,1116,1180,1208,1298,1338,1407,1641,1643,1659,3216,4006
17/3 tagged:1169,1180,1184,1188,1190,1192,3216,3222,3778,3900,3999

- **Router de border del cliente CE**

En el CE como ya se tenía configurado anteriormente las VRF para datos e internet se precedió a destaguear las vlans de cada servicio en la interfaz GigabitEthernet0/2 de la siguiente manera.

Se levantó la interfaz física GigabitEthernet0/2 y se colocó una descripción a la misma.

URBANO_EXPRESS_DATOS(config)#interface GigabitEthernet0/2
URBANO_EXPRESS_DATOS(config-if)description
ENLACES_BK_DATOS_INTERNET_CORECESS
URBANO_EXPRESS_DATOS(config-if)#no shutdown

En la interfaz virtual GigabitEthernet0/2.3216 se destagueo la vlan para el servicio de datos, también se configuró la VRF y la IP designada.

URBANO_EXPRESS_DATOS(config)#interface GigabitEthernet0/2.3216
URBANO_EXPRESS_DATOS(config-if)description
DATOS_BK_CORECESS_PE.170

URBANO_EXPRESS_DATOS(config-if)encapsulation dot1Q 3216
URBANO_EXPRESS_DATOS(config-if)#ip vrf forwarding datos
URBANO_EXPRESS_DATOS(config-if)#ip address 10.1.239.6 255.255.255.252
URBANO_EXPRESS_DATOS(config-if)#no shutdown

En la interfaz virtual GigabitEthernet0/2.3222 se destagueo la vlan para el servicio de internet, también se configuró la VRF y la ip designada.

URBANO_EXPRESS_DATOS(config)#interface GigabitEthernet0/2.3222
URBANO_EXPRESS_DATOS(config-if)description
INTERNET_BK_CORECESS_PE.170
URBANO_EXPRESS_DATOS(config-if)encapsulation dot1Q 3222
URBANO_EXPRESS_DATOS(config-if)#ip vrf forwarding internet
URBANO_EXPRESS_DATOS(config-if)#ip address 192.168.43.38
255.255.255.252
URBANO_EXPRESS_DATOS(config-if)#no shutdown
Cabe mencionar que en una interfaz sea física o virtual no se puede configurar más de una VRF y también primero se tiene que asociar la VRF la interfaz para posteriormente configurar la IP correspondiente.

Con el procesó realizado ya se tiene conectividad desde el PE hacia el CE y viceversa.

PE Backup hacia el CE
PE03#ping vrf dat1010 10.10.10.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

PE03#ping vrf internet 192.168.43.38
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.43.38, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CE hacia el PE Backup

URBANO_EXPRESS_DATOS#ping vrf datos 10.10.10.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

URBANO_EXPRESS_DATOS#ping vrf internet 192.168.43.37
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.43.37, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

3.1.1.3 Configuración de BGP en el CE

Una vez que ese tubo conectividad tanto el enlace principal y backup se procedió configurar el protocolo BGP para dar prioridad al enlace principal sobre el backup mediante el local_prefen y el as_path.

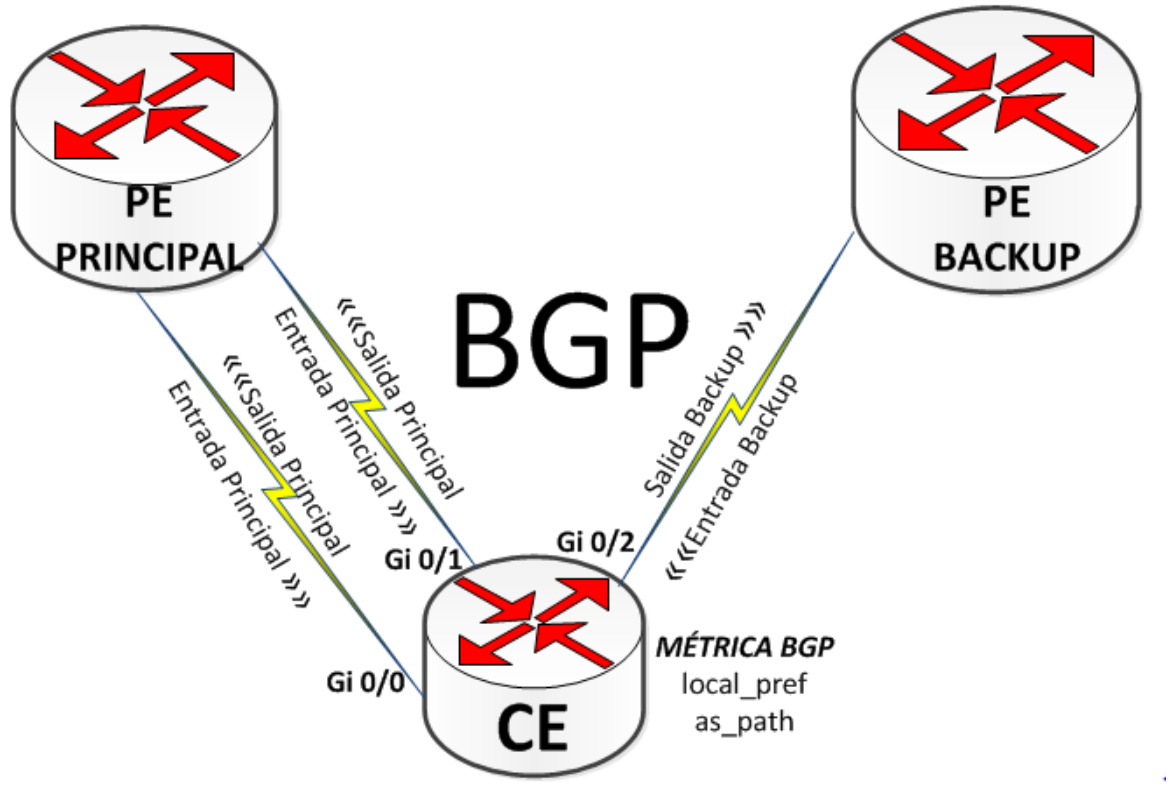

Figura 38. BGP entre PE principal, backup y CE

- **PE PRINCIPAL BGP**

Se configuró en el PE principal dentro de las sesiones BGP y la VRF correspondiente del enlace de datos e internet de la siguiente manera.El número de sistema autónomo local para el enlace de datos es el 56001 en la VRF dat1010 definida en la address family de ipv4, el sistema autónomo remoto es el 64514 más adelante configurará en el CE con el vecindad 10.10.10.2, también se activada el vecino correspondiente y con el override permitimos llegar a subredes que tengan el mismo sistema autónomo de BGP, como este enlace es de matriz concentrador de internet se difunde la ruta por defecto por la red MPLS al resto de PE para que las subredes puedan salir hacia el internet por medio de la red de datos, las configuraciones realizadas se detalla a continuación:

PE02(config)#router bgp 56001
PE02(config-router)address-family ipv4 vrf dat1010

PE02(config-router-af)#neighbor 10.10.10.2 remote-as 64514
PE02(config-router-af)#neighbor 10.10.10.2 description
URBANO_EXPRESS_PRINCIPAL_DATOS
PE02(config-router-af)#neighbor 10.10.10.2 activate
PE02(config-router-af)#neighbor 10.10.10.2 as-override
PE02(config-router-af)#default-information originate
PE02(config-router-af)#network 10.10.10.0 mask 255.255.255.252

El número de sistema autónomo local para el enlace de internet es el 56001 en la VRF internet definida en la address family de ipv4, el sistema autónomo remoto es el 64700 más adelante configurará en el CE con el vecindad 192.168.43.42, también se activada el vecino correspondiente, se difunde la ruta por defecto con el vecino correspondiente y se realiza un filtro con una lista de prefijos para que solo aprenda la ruta por defecto y no otras rutas.

PE02(config)#router bgp 56001
PE02(config-router)address-family ipv4 vrf internet
PE02(config-router-af)# neighbor 192.168.43.42 remote-as 64700
PE02(config-router-af)# neighbor 192.168.43.42 description
URBANO_EXPRESS_MATRIZ_INTERNET_MPLS_PRINCIPAL
PE02(config-router-af)# neighbor 192.168.43.42 activate
PE02(config-router-af)# neighbor 192.168.43.42 default-originate
PE02(config-router-af)# neighbor 192.168.43.42 prefix-list
ONLY_DEFAULT_ROUTE out

La lista de prefijos es la siguiente que permite aprender solo la ruta por defecto y se aplica para el tráfico de salida del PE.

ip prefix-list ONLY_DEFAULT_ROUTE seq 5 permit 0.0.0.0/0
ip prefix-list ONLY_DEFAULT_ROUTE seq 10 deny 0.0.0.0/0 ge 1

- **PE BACKUP BGP**

Se configuró en el PE backup dentro de las sesiones BGP y la VRF correspondiente del enlace de datos e internet de la siguiente manera.

El número de sistema autónomo local para el enlace de datos es el 56001 en la VRF dat1010 definida en la address family de ipv4, el sistema autónomo remoto es el 64514 más adelante configurará en el CE con el vecindad 10.10.10.6, también se activada el vecino correspondiente y con el override permitimos llegar a subredes que tengan el mismo sistema autónomo de BGP, como este enlace es de matriz concentrador de internet backup se difunde la ruta por defecto por la red MPLS al resto de PE para que las subredes puedan salir hacia el internet por medio de la red de datos, las configuraciones realizadas se detalla a continuación:

PEO3(config)#router bgp 56001
PEO3(config-router)address-family ipv4 vrf dat1010
PEO3(config-router-af)#neighbor 10.10.10.6 remote-as 64514
PEO3(config-router-af)#neighbor 10.10.10.6 description
URBANO_EXPRESS_BK_DATOS
PEO3(config-router-af)#neighbor 10.10.10.6 activate
PEO3(config-router-af)#neighbor 10.10.10.6 as-override
PEO3(config-router-af)#default-information originate
PEO3(config-router-af)#network 10.10.10.4 mask 255.255.255.252

El número de sistema autónomo local para el enlace de internet es el 56001 en la VRF internet definida en la address family de ipv4, el sistema autónomo remoto es el 64700 más adelante configurará en el CE con el vecindad 192.168.43.42, también se activada el vecino correspondiente, se difunde la ruta por defecto con el vecino correspondiente y se realiza un filtro con una lista de prefijos para que solo aprenda la ruta por defecto y no otras rutas. PE03(config)#router bgp 56001

PE03(config-router)address-family ipv4 vrf internet
PE03(config-router-af)# neighbor 192.168.43.38 remote-as 64700
PE03(config-router-af)# neighbor 192.168.43.38 description
URBANO_EXPRESS_MATRIZ_INTERNET_MPLS_BK
PE03(config-router-af)# neighbor 192.168.43.38 activate
PE03(config-router-af)# neighbor 192.168.43.38 default-originate
PE03(config-router-af)# neighbor 192.168.43.38 prefix-list
ONLY_DEFAULT_ROUTE out

La lista de prefijos es la siguiente que permite aprender solo la ruta por defecto y se aplica para el tráfico de salida del PE de backup.

ip prefix-list ONLY_DEFAULT_ROUTE seq 5 permit 0.0.0.0/0
ip prefix-list ONLY_DEFAULT_ROUTE seq 10 deny 0.0.0.0/0 ge 1

- **Router Border Cliente CE**

En el CE se procedió activar el protocolo BGP para definir el enlace principal y de backup, se configuró las métricas de local_prefer y el as_path, para el servicio de datos se tiene un sistema autónomo y para el enlace de internet otro sistema autónomo. La sesión BGP se creó con el sistema autónomo designado para datos que es el 64514, la IPv4 del enlace principal fue configurada como el identificar del router en la sesión BGP, también se habilito los log que exista en las vecindades BGP y permita crear varias familias ipv4, estas configuraciones sirven para los dos servicios de datos y acceso a internet.

URBANO_EXPRESS_DATOS(config)#router bgp 64514
URBANO_EXPRESS_DATOS(config-router)#bgp router-id 10.10.10.2
URBANO_EXPRESS_DATOS(config-router)#bgp log-neighbor-changes
URBANO_EXPRESS_DATOS(config-router)#no bgp default ipv4-unicast

El resto de configuraciones del protocolo BGP se divide en cuatro partes que son:

1. Enlace principal datos
2. Enlace backup datos
3. Enlace principal internet
4. Enlace backup internet

Las configuraciones se realizaron en el orden que se presenta a continuación:

- **BGP enlace principal de datos CE**

Para designar el enlace principal del backup cómo se mencionó anteriormente se configuraron políticas (route-map). Las política que se creó es para los enlaces de

datos e internet para las subredes de entrada al CE, esta política tiene el nombre de entrada principal configurado un local-preference de 350.

URBANO_EXPRESS_DATOS(config)#route-map entrada_principal permit 10
URBANO_EXPRESS_DATOS(config-route-map)#set local-preference 350
URBANO_EXPRESS_DATOS(config-route-map)#exit
URBANO_EXPRESS_DATOS(config)#route-map entrada_principal deny 20

Se creó una política de salida de las subredes del CE para el enlace principal de datos, esta política tiene el nombre de salida principal configurada con un path de dos sistemas autónomos aunque solo se aumenta un AS el prepend cuenta como un AS extra.

URBANO_EXPRESS_DATOS(config)#route-map salida_principal_datospermit 10
URBANO_EXPRESS_DATOS(config-route-map)#set as-path prepend 64514
URBANO_EXPRESS_DATOS(config-route-map)#exit
URBANO_EXPRESS_DATOS(config)#route-map salida_principal_datos deny 20

Una vez creada las políticas se procedió en el address-family ipv4 de la VRF de datos a realizar las siguientes configuraciones: definir el sistema autónomo remoto que es el 56001 relacionado con su vecino, activar la vecindad del enlace principal, habilitar el allowas-in para llegar hacia las subredes de las sucursales que tienen el mismo sistema autónomo de matriz, generalmente BGP restringe comunicaciones entre similares AS para no generar lasos en la red pero en nuestro caso se necesita que subredes del mismo AS se puedan comunicar, también se relaciona las políticas creadas de entrada y de salida con su respectivas vecindades.

URBANO_EXPRESS_DATOS(config)#router bgp 64514
URBANO_EXPRESS_DATOS(config-router)# address-family ipv4 vrf datos
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.1 remote-as 65001
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.1 description PRINCIPAL_PE.175
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.1 activate
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.1 allowas-in

URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.1 route-map entrada_principal in
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.1 route-map salida_principal_datos out

- **BGP enlace backup de datos CE**

La política que se creó para el enlace de backup de datos e internet para las subredes de entrada al CE tiene el nombre de entrada backup configurado con un local-preference de 200 brindando una preferencia local menor que el enlace principal que tiene de 350 lo que permitió definir entre enlace principal y backup.

URBANO_EXPRESS_DATOS(config)#route-map entrada_bk permit 10
URBANO_EXPRESS_DATOS(config-route-map)#set local-preference 200
URBANO_EXPRESS_DATOS(config-route-map)#exit
URBANO_EXPRESS_DATOS(config)#route-map entrada_bk deny 20

Se creó una política de salida de las subredes del CE para el enlace de backup de datos, esta política tiene el nombre de salida backup datos configurada con un path de cuatro sistemas autónomos aunque solo se aumenta tres AS el prepend cuenta como un AS extra, detectando como un camino con mayor saltos comparada al enlace de dos AS por lo que elige como una ruta de backup.

URBANO_EXPRESS_DATOS(config)#route-map salida_BK_datos permit 10
URBANO_EXPRESS_DATOS(config-route-map)#set as-path prepend 64514 64514 64514
URBANO_EXPRESS_DATOS(config-route-map)#exit
URBANO_EXPRESS_DATOS(config)#route-map salida_BK_datos deny 20

Una vez creada las políticas se procedió en el address-family ipv4 de la VRF de datos a realizar las siguientes configuraciones: definir el sistema autónomo remoto que es el 56001 relacionado con su vecino, activar la vecindad del enlace principal, habilitar el allowas-in para llegar hacia las subredes de las sucursales que tienen el mismo sistema autónomo de matriz, también se relaciona las políticas creadas de entrada y de salida con su respectivas vecindades

URBANO_EXPRESS_DATOS(config)#router bgp 64514
URBANO_EXPRESS_DATOS(config-router)# address-family ipv4 vrf datos
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.5 remote-as 65001
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.5 description BK_PE.170
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.5 activate
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.5 allowas-in
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.5 route-map entrada_bk in
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 10.10.10.5 route-map salida_BK_datos out

Con las configuraciones antes realizadas ya se tiene funcionando correctamente y levantado la sesión BGP el enlace datos tanto principal como bakup esto se puede comprobar con el comando show ip bgp vpnv4 de la VRF.

URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#sh ip bgp vpnv4 vrf datos summary | inc 10.10.10
GP router identifier 10.10.10.2, local AS number 64514
10.10.10.1 4 56001 23000 22976 120 0 0 2w0d 19
10.10.10.5 4 56001 22000 19009 1 0 0 2wod 19
URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#

- **BGP Enlace principal de internet CE**

Para el enlace de internet principal para el tráfico de entrada se utilizó la política antes creada que tiene el nonmbre de entrada_principal con un local preference de 350. Se creó una política de salida de las subredes del CE para el enlace principal de internet, esta política tiene el nombre de salida principal internet configurada con un path de dos sistemas autónomos aunque solo se aumenta un AS 64700 el prepend cuenta como un AS extra.

URBANO_EXPRESS_DATOS(config)#route-map salida_principal_internet permit 10
URBANO_EXPRESS_DATOS(config-route-map)#set as-path prepend 64700
URBANO_EXPRESS_DATOS(config-route-map)#exit
URBANO_EXPRESS_DATOS(confi)#route-map salida_principal_internet deny 20

Una vez creada las políticas se procedió en el address-family ipv4 de la VRF de internet a realizar las siguientes configuraciones: definir el sistema autónomo remoto que es el 56001 relacionado con su vecino, activar la vecindad del enlace principal, definir el sistema autónomo local debido que es diferente al de datos, , también se relaciona las políticas creadas de entrada y de salida con su respectivas vecindades.

URBANO_EXPRESS_DATOS(config)#router bgp 64514
URBANO_EXPRESS_DATOS(config-router)# address-family ipv4 vrf internet
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.41 remote-as 65001
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.41 description PRINCIPAL_PE.175
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.41 activate
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.41 local-as 64700
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.41 route-map entrada_principal in
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.41 route-map salida_principal_internet out

- **BGP enlace backup de internet CE**

La política del enlace de backup de datos e internet para las subredes de entrada al CE ya se configuró anteriormente que tiene el nombre de entrada backup configurado con un local-preference de 200 brindando una preferencia local

menor que el enlace principal que tiene de 350 lo que permitió definir entre enlace principal y backup.

Se creó una política de salida de las subredes del CE para el enlace de backup de internet, esta política tiene el nombre de salida backup internet configurada con un path de cuatro sistemas autónomos aunque solo se aumenta tres AS 64700 el prepend cuenta como un AS extra, detectando como un camino con mayor saltos comparada al enlace de dos AS por lo que elige como una ruta de backup.

URBANO_EXPRESS_DATOS(config)#route-map salida_BK_internet permit 10
URBANO_EXPRESS_DATOS(config-route-map)#set as-path prepend 64700 64700 64700
URBANO_EXPRESS_DATOS(config-route-map)#exit
URBANO_EXPRESS_DATOS(config)#route-map salida_BK_internet deny 20

Una vez creada las políticas se procedió en el address-family ipv4 de la VRF de internet se realizó las siguientes configuraciones: definir el sistema autónomo remoto que es el 56001 relacionado con su vecino, activar la vecindad del enlace backup, definir el sistema autónomo local, también se relaciona las políticas creadas de entrada y de salida con su respectivas vecindades.

URBANO_EXPRESS_DATOS(config)#router bgp 64514
URBANO_EXPRESS_DATOS(config-router)# address-family ipv4 vrf internet
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.37 remote-as 65001
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.37 description BK_PE.170
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.37 activate
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.37 local-as 64700
URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.37 route-map entrada_bk in

URBANO_EXPRESS_DATOS(config-router-af)#neighbor 192.168.43.37 route-map salida_BK_internet out

Con las configuraciones antes realizadas ya se tiene funcionando correctamente y levantado la sesión BGP el enlace internet tanto principal como bakup esto se puede comprobar con el comando show ip bgp vpnv4 de la VRF internet.

URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#sh ip bgp vpnv4 vrf internet summary | inc 192.168.43
GP router identifier 10.10.10.2, local AS number 64700
192.168.43.41 4 56001 23000 22346 120 0 0 2w0d 8
192.168.43.37 4 56001 23056 23064 1 0 0 2wod 8
URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#

Todas las configuraciones que se realizaron anteriormente en el CE tiene un propósito que es la comunicación de la WAN. Para la LAN de datos se utilizó una subred de IPs privadas con máscara de 24 bits y la LAN de internet una subred pública con máscara de 30 bits, la cual, se conecta al firewall que administra el acceso a internet de las sucursales, este firewall tiene una conexión directa a una interfaz del router virtualizado de datos, en esta comunicación se estableció una subred privada de máscara de 30 bits, con esta conexión garantizamos que el tráfico de la red interna no colapse por las peticiones que realicen simultáneamente los host para datos e internet.

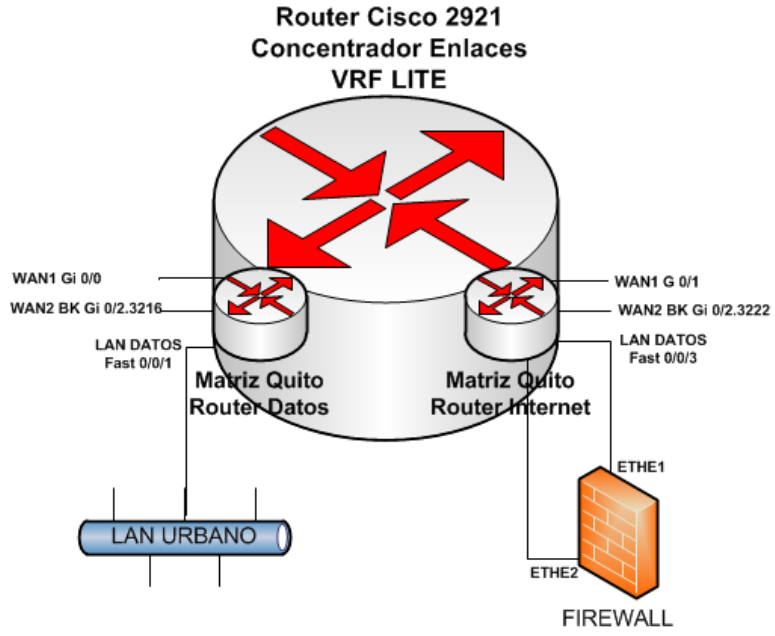

Figura 39. Esquema del CE hacia la LAN.

a) En la figura número 38 se evidencia las conexiones que se realizaron en la LAN.

A continuación se detallara las configuraciones implementadas:

La subred LAN de datos es la 192.168.1.0/24 configurada en la interfaz VLAN número 20 que se asoció a la VRF de datos y se asignó a la interfaces FastEthernet0/0/0 y FastEthernet0/0/1 en donde se conecta la red interna.

URBANO_EXPRESS_DATOS(config)#interface vlan 20
URBANO_EXPRESS_DATOS(config-if)#description LAN_DATOS
URBANO_EXPRESS_DATOS(config-if)#ip vrf forwarding datos
URBANO_EXPRESS_DATOS(config-if)#ip address 192.168.1.7 255.255.255.0
URBANO_EXPRESS_DATOS(config-if)#no shutdown

Antes de asignar la VLAN en la interfaz correspondiente se procedió activar la vlan en el database del router cisco de la siguiente manera.

URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#vlan database

URBANO_EXPRESS_DATOS(vlan)#vlan 10
VLAN 10 modified:
URBANO_EXPRESS_DATOS(vlan)#vlan 11
VLAN 11 modified:
URBANO_EXPRESS_DATOS(vlan)#vlan 20
VLAN 20 modified

Cabe mencionar que se activó las VLAN utilizadas para la LAN de datos (VLAN 20), IP pública de internet (VLAN 10) y la VLAN 11 para la conexión con el firewall. En las interfaces FastEthernet0/0/0 y FastEthernet0/0/1 se asignó la VLAN 20 en modo acceso, cabe mencionar que son interfaces de capa 2 y por defecto su funcionamiento se encuentra en modo acceso, se añadió una descripción y se activó la misma, como se muestra a continuación:

URBANO_EXPRESS_DATOS(config)#interface FastEthernet0/0/0
URBANO_EXPRESS_DATOS(config-if)#switchport access vlan 20
URBANO_EXPRESS_DATOS(config-if)# description LAN_DATOS
URBANO_EXPRESS_DATOS(config-if)#no shutdown

URBANO_EXPRESS_DATOS(config)#interface FastEthernet0/0/1
URBANO_EXPRESS_DATOS(config-if)#switchport access vlan 20
URBANO_EXPRESS_DATOS(config-if)# description LAN_DATOS
URBANO_EXPRESS_DATOS(config-if)#no shutdown

La conexión entre CE y el firewall se utilizó la subred 10.10.10.0/30 configurada en la interfaz VLAN número 11 que se asoció a la VRF de datos y se asignó a la interfaz FastEthernet0/0/2 donde se conecta el firewall, las configuraciones para esta VLAN e interfaz son las siguientes:

URBANO_EXPRESS_DATOS(config)#interface vlan 11
URBANO_EXPRESS_DATOS(config-if)#description LAN_SALIDA_INTERNET
URBANO_EXPRESS_DATOS(config-if)#ip vrf forwarding datos
URBANO_EXPRESS_DATOS(config-if)#ip address 20.20.20.1 255.255.255.252
URBANO_EXPRESS_DATOS(config-if)#no shutdown

URBANO_EXPRESS_DATOS(config)#interface FastEthernet0/0/2
URBANO_EXPRESS_DATOS(config-if)#switchport access vlan 11
URBANO_EXPRESS_DATOS(config-if)# description LAN_SALIDA_INTERNET
URBANO_EXPRESS_DATOS(config-if)#no shutdown

En la conexión con la LAN de firewall y el CE se estableció la ruta por defecto para que todas las sucursales puedan acceder al internet mediante el servicio de internet de matriz, en el firewall se permite o se deniega las subredes que pueden navegar en el internet, la IP 20.20.20.2 se encuentra configurada en la interfaz del firewall.

URBANO_EXPRESS_DATOS(config)#ip route vrf datos 0.0.0.0 0.0.0.0 20.20.20.2
En la salida al internet se utilizó la subred 181.49.11.0/30 configurada en la interfaz VLAN número 10 que se asoció a la VRF de internet y se asignó a la interfaz FastEthernet0/0/3 donde se conecta a la IP pública del firewall, las configuraciones para esta VLAN e interfaz son las siguientes:

URBANO_EXPRESS_DATOS(config)#interface vlan 10
URBANO_EXPRESS_DATOS(config-if)#description
POOL_PUBLICAS_INTERNET
URBANO_EXPRESS_DATOS(config-if)#ip vrf forwarding internet
URBANO_EXPRESS_DATOS(config-if)#ip address 181.49.11.1 255.255.255.252

Todas estas IPs y rutas que se encuentran en la red interna (LAN) del CE son difundidas en su respectivas address family las cuales son datos e internet de la sesión BGP con el fin que las sucursales puedan llegar a las aplicaciones y acceso a internet que proporciona matriz.

En el address family de datos se procedió a configurar la red, redistribuir las rutas estáticas y la ruta por defecto para que las sucursales alcancen el internet, la subred 20.20.20.0/30 no se necesita publicar debido que es una conexión local.

URBANO_EXPRESS_DATOS(config)#router bgp 64514
URBANO_EXPRESS_DATOS(config-router)# address-family ipv4 vrf datos

URBANO_EXPRESS_DATOS(config-router-af)#network 192.168.1.0
URBANO_EXPRESS_DATOS(config-router-af)#redistribute static
URBANO_EXPRESS_DATOS(config-router-af)#default-information originate

En el address family de internet se procedió a configurar la subred pública designada con su respectiva máscara.

URBANO_EXPRESS_DATOS(config)#router bgp 64514
URBANO_EXPRESS_DATOS(config-router)# address-family ipv4 vrf internet
URBANO_EXPRESS_DATOS(config-router-af)#network 181.49.11.0 mask 255.255.255.252

3.1.2 Concentrador Guayaquil

En la ciudad de Guayaquil se encuentra el concentrador de acceso a internet backup de las sucursales a nivel nacional, este concentrador tiene una configuración similar al concentrador de Quito, tiene dos últimas millas: fibra óptica enlace principal y radio enlace como backup, está configurado a dos PEs y tiene un solo router CE el cual realiza VRF lite para los servicios de datos y acceso a internet, se empleó 4 VLANs, dos subredes privadas con mascara de treinta bits y una subred pública con máscara de treinta bits y el protocolo BGP a nivel de WAN para la comunicación de enlace principal y backup entre el PE y CE.

La principal diferencia en el protocolo BGP que se implementó en la métrica de as_path para distribuir la salida al internet hacia las sucursales se aumentó a 6 AS del enlace principal y de 8 AS el enlace de backup, con esto se consiguió que la primera opción de acceso a internet de las sucursales sea por matriz Quito enlaces principal (as_path= 2 AS), segundo matriz Quito enlace backup (as_path=4 AS), tercera matriz Guayaquil enlace principal (as_path=6) y la cuarta opción es matriz Guayaquil enlace backup (as_path=8) todas estas conmutaciones son automáticas mediante el protocolo BGP.

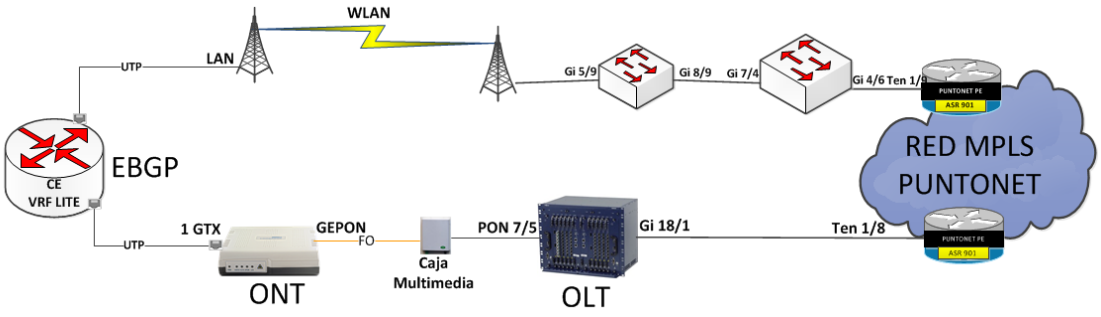

Figura 40. Topología de red MPLS Matriz Guayaquil

3.2 Instalación de enlace principal de las sucursales

Todas las sucursales a nivel nacional se configuraron de similar forma, es decir, un enlace de datos con acceso a internet mediante matriz Quito o Guayaquil, para estos enlaces se implementó dos últimas milla generalmente fibra óptica el enlace principal y radio enlace, ADSL o VSAT como enlace de backup.

A continuación se presenta la configuración desde el PE hasta el CE que se realizó para el enlace principal de las sucursales a nivel nacional, la topología implementada también es similar para facilitar el soporte técnico.

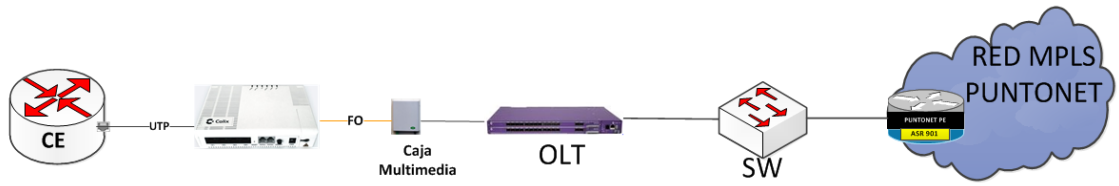

Figura 41. Topología enlace principal sucursales

Para realizar las configuraciones a la nueva tecnología MPLS se utilizó los mismos recursos que ya se tenía con la red Ethernet, aunque en determinados punto se realizó un cambio del router CE y patch de cobre, el momento que se realizaba la migración se suspendió el servicio alrededor de 30 minutos, este tiempo es corto debido que se realizó un análisis anterior de la topología, direccionamiento y enrutamiento cada uno de las sucursales, en este análisis se verificaba por todos los equipos que pasaba el enlace como SW core, SW intermedios, OLT, ONT y CE.

3.2.1 Activación de la Vlan

Los enlaces utilizan una VLAN para la comunicación entre el PE y CE por tal motivo esta VLAN se pasó por todos los equipos como Sw core, SW intermedios, OLT y en el ONT que entrega en mod acceso la VLAN al CE.

3.2.1.1 PE

En los PEs existe dos formar de activar la VLAN, esto depende de las configuraciones del PE.

En determinados PEs se tiene que realizar mediante una instancia de servicio (service instance), esta instancia de servicio se configura en el puerto en el cual se conecta con el SW core o en algunos casos la interfaz que se conecta directamente con el OLT. En la instancia de servicio se define la interfaz en la cual se va activar la VLAN, el número de la instancia, una descipción, la VLAN la cual se va encapsular además de activar también se taguea la VLAN y definir que es un servicio de capa 3 con el bridge domain de la VLAN.

PE08(config)#interface Gi 0/2
PE08(config-if)#service instance 61 ethernet
PE08(config-if-srv)#description URBANO_EXPRESS_COCA
PE08(config-if-srv)#encapsulation dot1q 61
PE08(config-if-srv)#rewrite ingress tag pop 1 symmetric
PE08(config-if-srv)#bridge-domain 61

En otros PEs se tiene que activar y taguear la VLAN en la base de datos correspondiente del equipo o cambiando el status de la VLAN.

3.2.1.2 Switch core e intermedios

Generalmente los puertos en switch de core las vlans se encuentran pasadas en rangos en modo trunk, por tal motivo, el momento que se active la vlan se verifica la misma pasada por diferentes puertos del switch causando lasos en la red y consumo de los recursos (memoria, cpu) de los equipo switch, para eliminar estos posibles inconvenientes se remueve la vlan de los puertos en los que no tendría que estar pasados.

La VLAN en el switching de core se activa en la base de datos de las VLANs de la siguiente manera.

SW-L3-COCA(vlan)#vlan 61
VLAN 61 modified

Una vez activa la VLAN para verificar los puertos en los cuales se encuentra pasada la misma, se realiza con el siguiente comando: show vlan id (número de la vlan)

SW-L3-COCA#show vlan id 61

VLAN	*Name*	*Status*	*Ports*
61	*VLAN61*	*active*	*Gi1/1, Gi1/5, Gi1/7, Gi1/17*
			Gi1/30, Gi1/42, Gi1/43, Gi1/47

Como se puede verificar en el resultado del comando show vlan id esta vlan se encuentra pasada por varios puertos que no tendría que estar, por tal motivo se procede a eliminar la vlan de los puertos erróneos.

Como buena práctica se recomienda antes de eliminar la vlan de la interfaz verificar las vlans que se encuentren pasadas en ese momento por la interfaz, esto debido que, si existe un error como borrar el resto de vlans pasadas en la interfaz puede volver a configurarles.
Verificó que las vlan que se encuentres pasadas en la interfaz GigabitEthernet 1/1.

SW-L3-COCA#sh run interface gigabitEthernet 1/1
Building configuration...
Current configuration : 329 bytes
!
interface GigabitEthernet1/1
description SW-Radio Terraza POrt 3
switchport trunk encapsulation dot1q

switchport trunk allowed vlan 2-68,70-73,75-79,81-106,108-116,118-882,884-1663
switchport trunk allowed vlan add 1665-4094
switchport mode trunk
load-interval 30
no cdp enable
spanning-tree guard root
end

Se ingresó a la interfaz para remover la vlan en la interfaz correcta.

SW-L3-COCA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-L3-COCA(config)# interface GigabitEthernet1/1
SW-L3-COCA(config-if)#switchport trunk allowed vlan remove 61

Por último, pero no menos importante, se verificó en la interfaz que la única vlan removida sea la 61.

SW-L3-COCA#sh run interface gigabitEthernet 1/1
Building configuration...
Current configuration : 329 bytes
!
interface GigabitEthernet1/1
description SW-Radio Terraza POrt 3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 2-60,62-68,70-73,75-79,81-106,108-116,118-882,884-1663
switchport trunk allowed vlan add 1665-4094
switchport mode trunk
load-interval 30
no cdp enable
spanning-tree guard root
end

Este mismo proceso se realizó en cada uno de la interfaces Gi1/1, Gi1/5, Gi1/7, Gi1/17 Gi1/30 y Gi1/42 en las cuales se encontraba pasada las vlans de forma inadecuada, al final este proceso se tiene activada y pasada en los dos únicas interfaces como se puede evidenciar.

SW-L3-COCA#show vlan id 61

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

61 VLAN61 active Gi1/43, Gi1/47

Este proceso se realiza en todos los switch de core e intermedios que se encuentran en la conexión entre el CE y PE.

3.2.1.3 OLT

En el OLT dependiendo de la marca del mismo se tiene dos opciones para crear y pasar la vlan por las interfaces PON y de UPLINK, para este enlace se emplea un OLT de marca Calix pero en otras sucursales se tiene de marca Corecess.

A continuación se detalla la activación de la VLAN para un OLT Calix.

Crear la vlan en el OLT Calix, en el item **VLANs**, la pestaña **PROVISIONING**, selecciona la pestaña **CREATE**, en la nueva ventana que presenta ingresamos en **ID** = Número de vlan a crear, **Name** = vlan_(Número de vlan) y activamos el **DHCP Snoop** = Activar posteriormente guardamos los cambios.

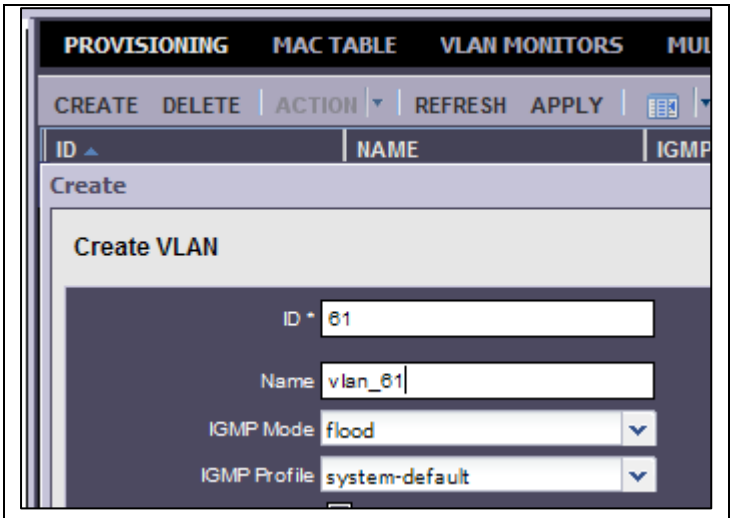

Figura 42. Creación de vlan en OLT Calix Coca

Una vez realizado el anterior paso se verifica en **VLANs --- PROVIONING** la vlan creada, seleccionamos la vlan con un doble clip para taggear en el puerto de uplink.

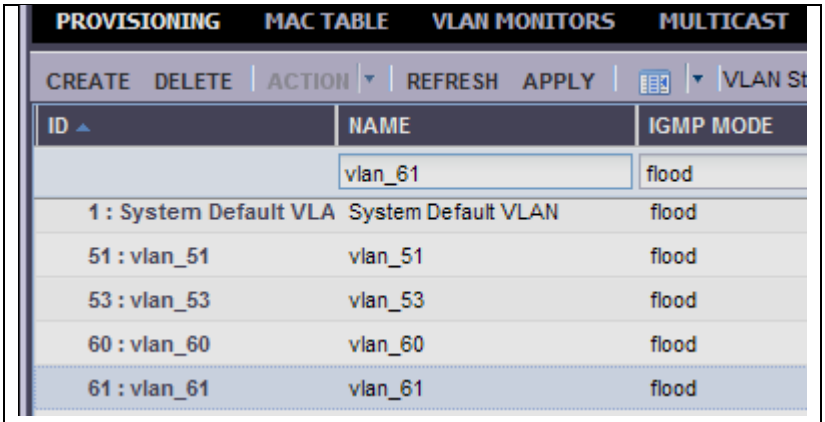

Figura 43. Listado de vlan en el OLT Calix Coca

Taggear la vlan en el puerto uplink, en el item **VLANs** en la pestaña **PROVISIONING** --- **ACTION** seleccionamos la opción **Add/Remove VLAN Members.**

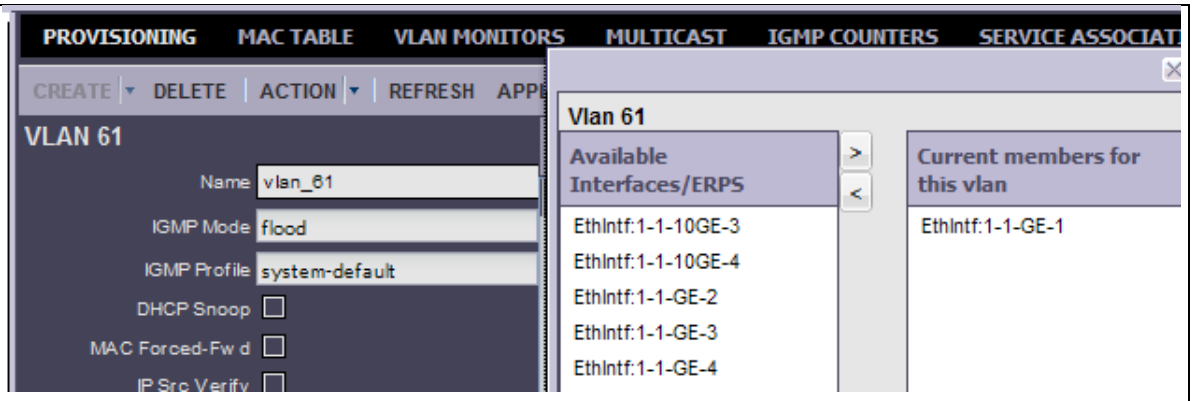

Figura 44. Taggerar la vlan en el puerto de UPLINK

En la figura 43 en la ventana seleccionamos el puerto UPLINK en el cual se taggera la vlan ejemplo la vlan 61 se taggea en el puerto ETHINTF: 1/1, con las fechas (> o <) **Add /Remove** el puerto seleccionado. En el puerto PON se activa el momento que se proporciona el servicio en el OLT no es necesario realizar el tagueo.

En los OLT de marca Corecess se taguear la vlan en el puerto de PON y de UPLINK de la siguiente manera.

Puerto GPON vlan datos e internet.
OLT-CUE-GPON(config)# dot1q port epon 1/2 tag 7070

Puerto de UPLINK vlan datos e internet
OLT-CUE-GPON (config)# dot1q port gigabitethernet 18/4 tag 7070

Cabe mencionar que estas configuraciones del OLT de marca Corecess son adquiridos de la sucursal de Cuenca que la última milla es fibra óptica.

3.2.2 Configuración en el ONT

Por en los enlaces principales generalmente la última milla es fibra óptica de marca Calix o Corecess depende de la ciudad en la cual se encuentra el enlace.

La configuración en cualquiera de las plataformas tienen los mismos parámetros a configurar como son: ancho de banda, nivel de compartición del enlace, número de la vlan, interfaz designada para el servicio y una descripción del enlace.

3.2.2.1 Corecess

En los ONT de marca Corecess las configuraciones se realiza por consola y generalmente se tiene 4 líneas de configuración indispensables para la conexión, en la primera se define si la vlan es dedicada o compartida (single o share), la segunda indica la vlan del circuito, las dos siguientes líneas se configura el ancho de banda de subida y de bajada como el nivel de compartición del enlace. Los cuatro parámetros antes mencionados están relacionados con el puerto epon y la Mac-Address del ONT.

port epon 1/2 link-mac 0090a3c85a20 bridge-mode single 64
port epon 1/2 link-mac 0090a3c85a20 tag-map single 61 0
port epon 1/2 link-mac 0090a3c85a20 up-bw 2048 2048 8 delay tolerant
port epon 1/2 link-mac 0090a3c85a20 down-bw 2048 2048 8 delay tolerant

En las líneas anteriores indica que el ONT se encuentra enganchado en el puerto epon 1/2 con la mac-address 0090a3c85a20 que representa el puerto 1GTX del ONT.

3.2.2.2 Calix

En los ONT de marca Calix se configura los mismos parámetros de un ONT marca corecess pero las configuraciones se realizó en modo gráfico, esta configuración se realiza en la siguiente secuencia, primero es el descubrimiento y provisionamiento del ONT y posteriormente activar los servicios en la interfaz indicada.

Un vez conectado el ONT CALIX, en el lapso de un minuto se engancha, físicamente se detecta que se enciende el led OPTICA POWER de color verde fijo, verificamos en el item **ONTs** en la pestaña **DISCOVERED ONTs** la FSAN SERIAL del ONT, selecciona la FSAN posteriormente escogemos en la pestaña **ACTION** en la opción **Link to new Provisioning.**

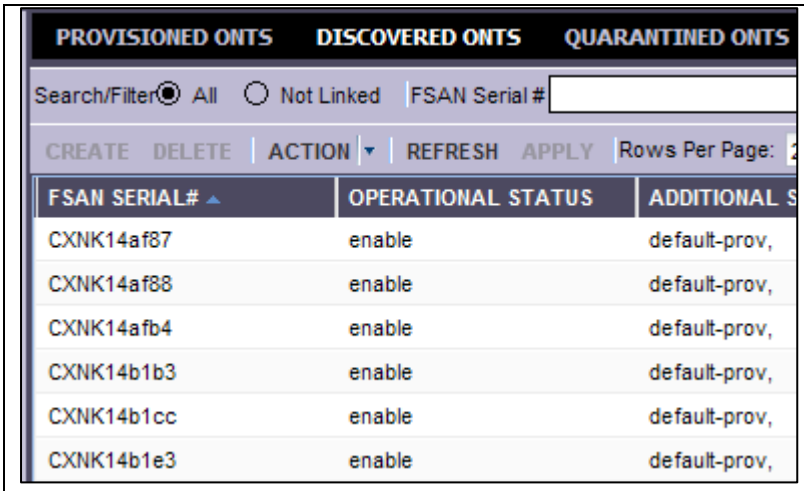

Figura 45. Descubrir un ONT Calix Coca

Mostrará una nueva ventana en el item **ONT PROFILE** selecciona el modelo del ONT en esta caso se usa el **T072G** y aceptamos el cambios **OK**.

Verificar ONT provisionado en el item **ONTs** la pestaña **PROVISIONED ONTS** == **PROVIONING** se verificó el número de ONT asignado a la FSAN. Ejemplo **ONT40** pertenece a la FSAN **14b4b7**, con esto evidenciamos que ya se encuentra pro visionado el ONT correctamente.

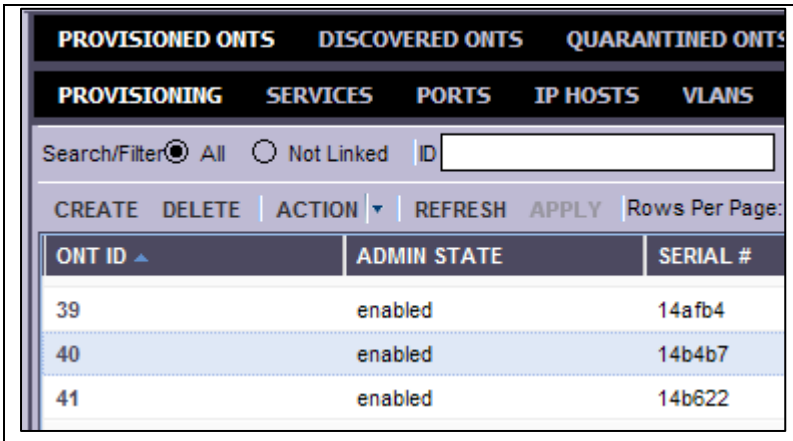

Figura 46. Designación del número de ONT Coca

Asignación de recursos en el ONT.- Se busca el ONT al cual se asignara los servicios dependiendo del puerto GPON al que se encuentra, en cada ONT se tiene los puertos GE1, GE2, GE3 y GE4, una vez seleccionado el ONT ejemplo el

ONT40, en la pestaña **SERVICES --- TABLE --- CREATE** escogemos la opción **Data Service**

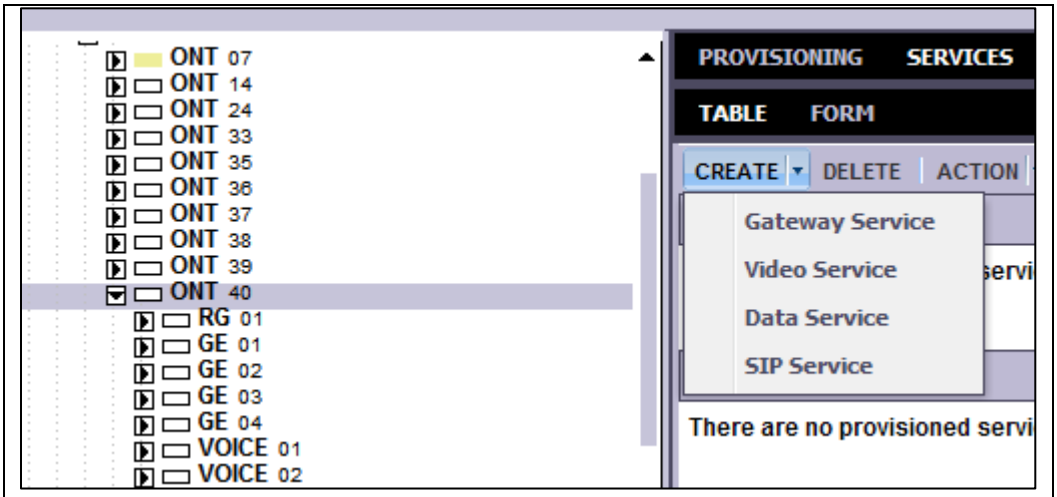

Figura 47. Selección del servicio en el ONT Calix Coca.

En la nueva ventana ingresamos los siguientes datos: **Subscriber Port** = El ONT tiene 4 port GigaEtherne, **Subscriber ID** = Codigo_Plan del netpus, Description = Nombre de la empresa en mayúsculas, **Service Name** = Data 1, **BW Profile** = Seleccionamos el AB de la lista que se creó anteriormente, **Service Tag Action** = Seleccionamos el Tag creado para cada vlan, **S-VLAN(Outer Tag)** = Número de VLAN presionamos **CREATE.**

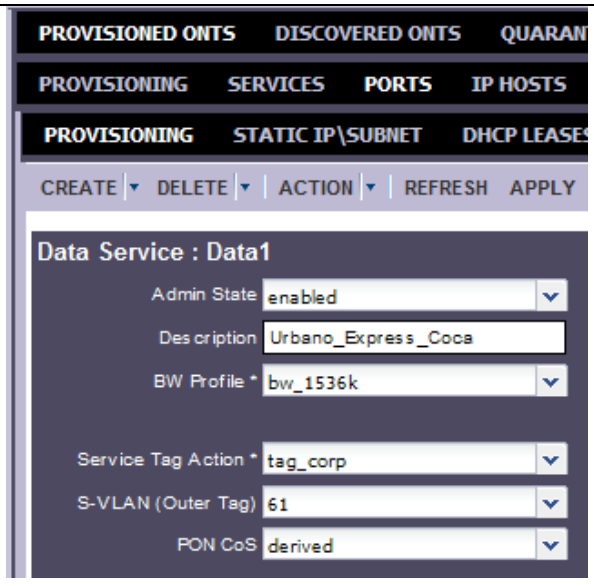

Figura 48. Recursos para el enlace de Datos Principal Coca

Los servicios creados en el ONT se encuentran en **ONT --- SERVICES --- TABLE** en el cual se confirma los datos como Puerto del ONT asignado, código_plan, nombre de la empresa, ancho de banda y vlan.

3.2.3 Configuración de direccionamiento IPv4

Para establecer la conexión entre el PE y CE se empleó una subred privada máscara de 30 bits para este caso la subred 10.10.10.192/30, por norma la IP impar válida para host de la subred se encuentra en el PE y la IP par es designada para el CE.

A continuación se detalla cómo se realizó la configuración en el PE y CE del direccionamiento ipv4.

3.2.3.1 PE

En el PE se creó la interfaz con el nombre de la vlan del circuito, en este caso la interface vlan 61. Pero con anterioridad se creó la VRF con el nombre de dat1010 única para la empresa Urbano Express en la red MPLS de Puntonet para los enlaces de datos.

PE08(config-vrf)#ip vrf dat1010

Se configuró el router distinguer en relación con el sistema autónomo de BGP y la VRF.

PE08(config-vrf)#rd 56001:1010

Importar y exportar los prefijos de la red e importa la vrf de monitoreo para alcanzar desde la intranet de Puntonet.

PE08(config-vrf)#route-target both 56001:1010

PE08(config-vrf)#route-target import 56001:888

Una vez creada y activada la VRF se procedió activar la interfaz VLAN correspondiente al enlace, la interface vlan 61 con su respectiva descripción, la VRF y la IP correspondiente.

PE08(config)#interface vlan 61

PE08(config-if)#description URBANO_EXPRESS_COCA

PE08(config-if)#ip vrf forwarding dat1010

PE08(config-if)#ip address 10.10.10.193 255.255.255.252
PE08(config-if)#no shutdown

3.2.3.2 CE

En el CE se procedió a realizar las configuraciones básicas y los accesos al router para administración y seguridad del equipo.
Se ingresó un nombre al router.
routers(config)#hostname URBANO_EXPRESS_COCA
URBANO_EXPRESS_COCA(config)#exit
URBANO_EXPRESS_COCA#

Se desactivó la búsqueda recurrente de dominios erróneos, evitando que el router se cuelgue temporalmente si se ingresa un comando erróneo.
URBANO_EXPRESS_COCA(config)#no ip domain lookup

Una contraseña de seguridad al momento de ingresar al mode de configuración global del router.
URBANO_EXPRESS_COCA(config)#enable secret wwwww

Seguridad al momento de ingresar por consola al cisco.
URBANO_EXPRESS_COCA(config)#line console 0
URBANO_EXPRESS_COCA(config-line)#password wwwww
URBANO_EXPRESS_COCA(config-line)#login

Un usuario local para la administración del router una vez activado el telnet, este usuario tiene privilegio 15 al cual no va pedir la contraseña para ingresar al modo de configuración global.
URBANO_EXPRESS_COCA(config)#username uwwwww privilege 15 password pwwwww

Se configuró el acceso al router mediante telnet con el usuario local.
URBANO_EXPRESS_COCA(config)#line vty 0 4
URBANO_EXPRESS_COCA(config-line)#login local

URBANO_EXPRESS_COCA(config-line)#transport input all

Se procedió a encriptar las contraseñas del router por seguridad,
URBANO_EXPRESS_COCA(config)#service password-encryption

Un mensaje de alerta si alguien quiere ingresar al router o para verificar a quien le pertenece el router.

URBANO_EXPRESS_COCA(config)#banner motd #

PUNTONET S.A.

Acceso restringido!!!

Solo personal autorizado - FC.

Fecha: 2015_10_15 E-mail: cccorporativo@puntonet.ec

Empresa: URBANO_EXPRESS_COCA

#

En la interface FastEthernet0/0 se configuró la IP del enlace principal para el enlace de datos.

URBANO_EXPRESS_COCA(config)#interface FastEthernet0/0
URBANO_EXPRESS_COCA(config-if)#description WAN_PNET
URBANO_EXPRESS_COCA(config-if)#ip address 10.10.10.194 255.255.255.252
URBANO_EXPRESS_COCA(config-if)#no shutdown

En la interface FastEthernet0/1 que fue designada para el enlace de internet se configuró la IP del enlace principal.

URBANO_EXPRESS_COCA(config)#interface FastEthernet0/1

URBANO_EXPRESS_COCA(config-if)#description LAN
URBANO_EXPRESS_COCA(config-if)#ip add 192.168.18.200 255.255.255.0
URBANO_EXPRESS_COCA(config-if)#no shutdown

Con estas configuraciones se obtuvo conectividad desde el PE hacia el CE y viceversa.

PE hacia el CE

PE02#ping vrf dat1010 10.10.10.194
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.194, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CE hacia el PE

URBANO_EXPRESS_COCA#ping vrf datos 10.10.10.193
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.193, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Nota: Las configuraciones del ONT de marca Corecess son recuperadas de la sucursal de Cuenca.

3.2.4 Configuración del protocolo BGP

Una vez que ese tubo conectividad en el enlace principal se procedió configurar el protocolo BGP en el PE y en el CE para proveer el servicio en la sucursal de manera inmediata y el tiempo de afectación sea el mínimo.

3.2.4.1 PE

Se configuró en el PE principal dentro de las sesiones BGP y la VRF correspondiente del enlace de datos con las siguientes consideraciones. El número de sistema autónomo local para el enlace de datos es el 56001 en la VRF dat1010 definida en la address family de ipv4, el sistema autónomo remoto es el 64514 más adelante configurará en el CE con el vecindad 10.10.10.194.

PE08(config)#router bgp 56001
PE08(config-router)address-family ipv4 vrf dat1010
PE08(config-router-af)#neighbor 10.10.10.194 remote-as 64514
PE08(config-router-af)#neighbor 10.10.10.194 description URBANO_EXPRESS_PRINCIPAL
PE08(config-router-af)#neighbor 10.10.10.194 activate
PE08(config-router-af)#neighbor 10.10.10.194 as-override
PE08(config-router-af)#network 10.10.10.0 mask 255.255.255.252

3.2.4.2 CE

Para designar el enlace principal del backup a nivel de la última milla se configuraron políticas (route-map). Las política que se creó es para las subredes de entrada al CE, esta política tiene el nombre de entrada principal configurado un local-preference de 350.

URBANO_EXPRESS_COCA(config)#route-map entrada_principal permit 10
URBANO_EXPRESS_ COCA(config-route-map)#set local-preference 350
URBANO_EXPRESS_ COCA(config-route-map)#exit
URBANO_EXPRESS_ COCA(config)#route-map entrada_principal deny 20

Se creó una política de salida de las subredes del CE para el enlace principal de datos, esta política tiene el nombre de salida principal configurada con un path de dos sistemas autónomos aunque solo se aumenta un AS el prepend cuenta como un AS extra.

URBANO_EXPRESS_COCA(config)#route-map salida_principal permit 10
URBANO_EXPRESS_COCA(config-route-map)#set as-path prepend 64514
URBANO_EXPRESS_COCA(config-route-map)#exit
URBANO_EXPRESS_COCA(config)#route-map salida_principal deny 20

Una vez creada las políticas se procedió a realizar las siguientes configuraciones: identificar del router, activar los log de BGP, permitir diferentes address family, definir el sistema autónomo remoto que es el 56001 relacionado con su vecino,

activar la vecindad del enlace principal, habilitar el allowas-in para llegar hacia las subredes matriz y resto de sucursales que tienen el mismo sistema autónomo, también se relaciona las políticas creadas de entrada y de salida con su respectivas vecindades y publicar la subred LAN por BGP.

URBANO_EXPRESS_COCA(config)#router bgp 64514
URBANO_EXPRESS_COCA(config-router)#bgp router-id 10.10.10.194
URBANO_EXPRESS_COCA(config-router)#bgp log-neighbor-changes
URBANO_EXPRESS_COCA(config-router)#no bgp default ipv4-unicast
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.193 remote-as 65001
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.193 description PRINCIPAL
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.193 activate
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.193 allowas-in
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.193 route-map entrada_principal in
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.193 route-map salida_principal out
URBANO_EXPRESS_COCA(config-router-af)#network 192.168.x.x

Con las configuraciones mencionadas el servicio de la sucursal ya está funcionando correctamente.

3.3 Instalación de enlace backup de las sucursales

3.3.1 Activación de la Vlan

Para cada enlace de backup se activa con una vlan la cual tiene que ser activado en los siguientes equipos:

3.3.1.1 PE Backup

La activación de la VLAN en el PE de backup se realizó mediante una instancia de servicio (service instance), la instancia de servicio se configuró en el puerto que conecta con el switch de core o intermedio. En la instancia de servicio se

define los siguientes parámetros: la interfaz que se va activar la VLAN, el número de la instancia, una descripción, la encapsulación, el tagueo y definir como un servicio de capa 3 con bridge domain.

Las configuraciones son las siguientes:

PE09(config)#interface Gi 0/0/1
PE09(config-if)#service instance 241 ethernet
PE09(config-if-srv)#description URBANO_EXPRESS_COCA_BK
PE09(config-if-srv)#encapsulation dot1q 241
PE09(config-if-srv)#rewrite ingress tag pop 1 symmetric
PE09(config-if-srv)#bridge-domain 241

3.3.1.2 Switch core

Se activó en el switch en la base de datos de las VLANs de la siguiente manera.
SW-L3-COCA(vlan)#vlan 241
VLAN 241 modified

Una vez activa la VLAN se verificó los puertos en los cuales se encuentra pasada mediante el siguiente comando: show vlan id (número de la vlan)

SW-L3-COCA#show vlan id 241

VLAN	*Name*	*Status*	*Ports*
241	*VLAN241*	*active*	*Gi1/1, Gi1/5, Gi1/7, Gi1/17*
			Gi1/30, Gi1/42, Gi1/43, Gi1/47

Como se puede verificar en el resultado del comando show vlan id esta vlan se encuentra pasada por varios puertos que no tendría que estar, por tal motivo se procede a eliminar la vlan de los puertos erróneos.

Como buena práctica se recomienda antes de eliminar la vlan de la interfaz verificar las vlans que se encuentren pasadas en ese momento por la interfaz, esto debido que, si existe un error como borrar el resto de vlans pasadas en la interfaz puede volver a configurarles. Verificó que las vlan que se encuentren pasadas en la interfaz GigabitEthernet 1/1.

SW-L3-COCA#sh run interface gigabitEthernet 1/1
Building configuration...
Current configuration : 329 bytes
!
interface GigabitEthernet1/1
description SW-Radio Terraza POrt 3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 2-68,70-73,75-79,81-106,108-116,118-882,884-1663
switchport trunk allowed vlan add 1665-4094
switchport mode trunk
load-interval 30
no cdp enable
spanning-tree guard root
end

Se ingresó a la interfaz para remover la vlan en la interfaz correcta.

SW-L3-COCA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-L3-COCA(config)# interface GigabitEthernet1/1
SW-L3-COCA(config-if)#switchport trunk allowed vlan remove 241

Por último, pero no menos importante, se verificó en la interfaz que la única vlan removida sea la 241.

SW-L3-COCA#sh run interface gigabitEthernet 1/1
Building configuration...
Current configuration : 329 bytes
!
interface GigabitEthernet1/1
description SW-Radio Terraza POrt 3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 2-60,62-68,70-73,75-79,81-106,108-116,118-882,884-1663

switchport trunk allowed vlan add 1665-240,242-4094
switchport mode trunk
load-interval 30
no cdp enable
spanning-tree guard root
end

Similar proceso se realizó en cada uno de las siguientes interfaces Gi1/1, Gi1/5, Gi1/7, Gi1/30, Gi1/43, Gi1/47 en las cuales se encontraba pasada las vlans de forma inadecuada, de esta manera se tiene activada y pasada en los dos únicas interfaces como se puede evidenciar.

SW-L3-COCA#show vlan id 241

VLAN	*Name*	*Status*	*Ports*
241	*VLAN241*	*active*	*Gi1/17, Gi1/42*

Este proceso se realiza en todos los switch de core e intermedios que se encuentran en la conexión entre el CE y PE.

3.3.1.3 Radio Base

La última milla con radio enlace la VLAN se pasa en modo troncal desde el switch de capa tres, switch intermedios hasta la radio base, por tal motivo, se procede a realizar las siguientes configuraciones en la radio base para activar la VLAN.

Las configuraciones se realizó a en modo gráfico empleando la herramienta de Mikrotik que es WinBox, en la opción lista de interfaces en la pestaña VLAN se procede a crear la vlan con el nombre de vlan241 y asociada a la interfaz ether1 que es la WAN de la radio base que se conecta al switch intermedio.

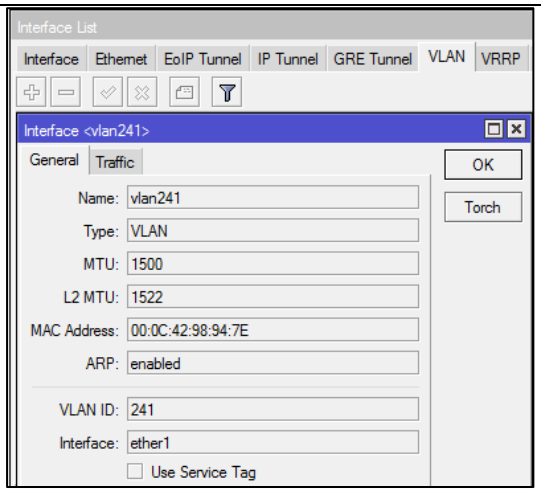

Figura 49. Crear la vlan en la radio base

Una vez creada la VLAN se procedió a crear el bridge con el nombre el mismo nombre.

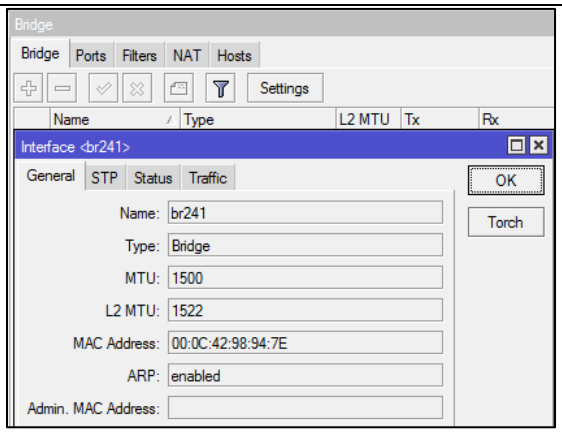

Figura 50. Crear el bridge en la radio base

A este bridge o puente se asocia la interface VLAN y el SSI de la radio remota, como se indica en el siguiente gráfico.

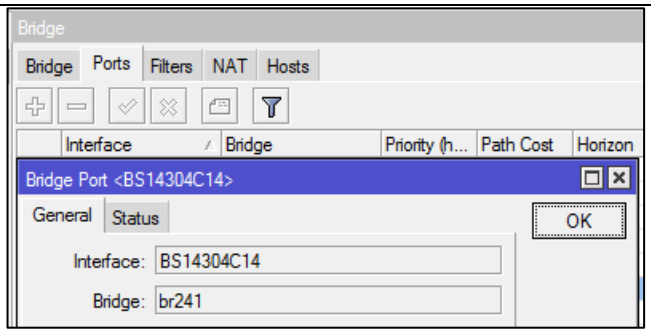

Figura 51. Asociar SSI a bridge en la radio base

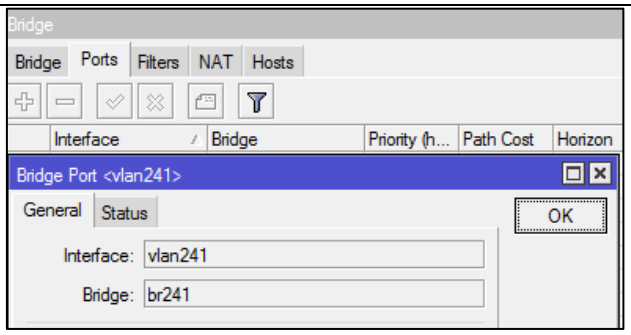

Figura 52. Asociar la interface VLAN al bridge

Con la asociación de las interfaces al bridge, la VLAN ya se encuentra activa y tagueada en las interfaces adecuadas para tener conexión.

3.3.2 Configuración última milla radio

Generalmente los enlaces que tiene la última milla radio enlace se procede a configurar un IP en la radio remota para administración, esta subred es de máscara de 29 bits, la primera IP se encuentra en la radio remota y la segunda en el switch de capa 3 asociadas a la misma VLAN del circuito.

3.3.2.1 Configuración de la Radio Base

En la base se procedió a crear un AP virtual con SSI BS14304C14, para poder crear el SSI se tiene que ingresar a la opción Wireless, luego agrega un AP Virtual con su respectivo nombre.

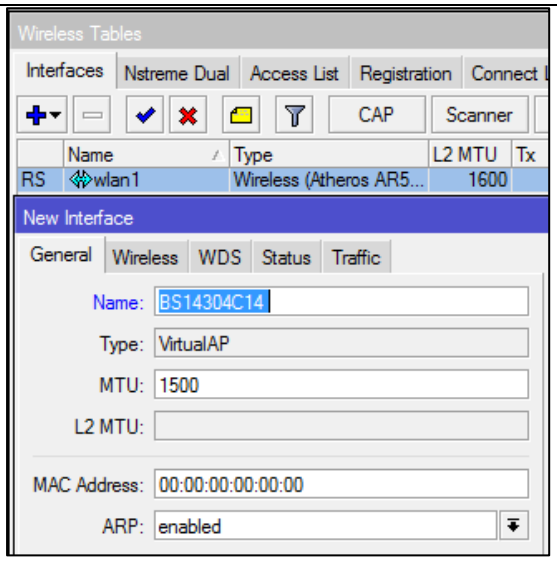

Figura 53. Creación del AP virtual

3.3.2.2 Configuración de la Radio Remota

La radio remota es de marca Mikrotik, de similar forma que la radio base en la opción Wireless se escanea los AP que se encuentra en el perímetro una vez detectado se establece una conexión entre radio y base. En la conexión que se establece entre los equipos antes mencionados se verifica algunos parámetros técnicos como el modo de operación, la banda, frecuencia, el canal y el SSI al cual se conectó.

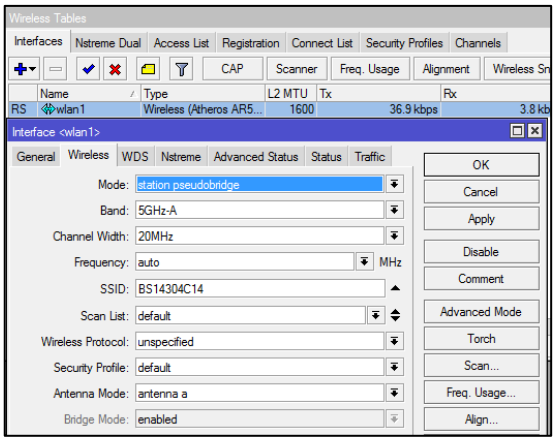

Figura 54. Establecer conexión radio base y radio remota

Como se mencionó anteriormente también se configura una IP para administración de la radio de la siguiente manera. La IP se encuentra asociada a la interfaz LAN ether1 de la radio remota.

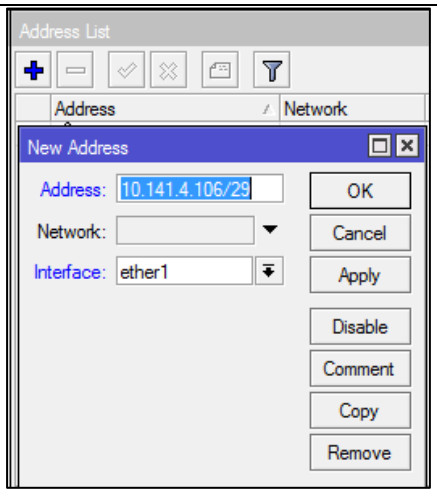

Figura 55. Configuración de IPv4 a la radio remota

3.3.2.3 Configuración en el SW-L3

El Gateway de la radio remota se creó en la interfaz vlan del circuito en el switch de capa 3, la máscara para este direccionamiento es 255.255.255.248 se utiliza una subred de 5 IPs disponibles para futuras pruebas de IP intermedia que se necesiten realizar en el soporte técnico.

La configuración es de la siguiente manera.

SW-L3-COCA(config)# interface vlan 241
SW-L3-COCA(config-if)#ip address 10.141.4.105 255.255.255.248
SW-L3-COCA(config-if)#no sh

3.3.3 Configuración del direccionamiento IPv4

Para establecer la conexión entre el PE y CE se empleó una subred privada de máscara de 30 bits para este caso la subred 10.10.10.192/30, por norma la IP impar válida para host de la subred se encuentra en el PE y la IP par es designada para el CE. A continuación se detalla cómo se realizó la configuración en el PE y CE del direccionamiento ipv4.

3.3.3.1 PE Backup

En el PE se creó la interfaz con el nombre de la vlan del circuito, en este caso la interface vlan 241. Pero con anterioridad se creó la VRF con el nombre de dat1010 única para la empresa Urbano Express en la red MPLS de Puntonet para los enlaces de datos.

PE09(config-vrf)#ip vrf dat1010

Se configuró el router distinguer en relación con el sistema autónomo de BGP y la VRF.

PE09(config-vrf)#rd 56001:1010

Importar y exportar los prefijos de la red e importa la vrf de monitoreo para alcanzar desde la intranet de Puntonet.

PE09(config-vrf)#route-target both 56001:1010

PE09(config-vrf)#route-target import 56001:888

Una vez creada y activada la VRF se procedió activar la interfaz VLAN correspondiente al enlace, la interface vlan 241 con su respectiva descripción, la VRF y la IP correspondiente.

PE09(config)#interface vlan 241

PE09(config-if)#description URBANO_EXPRESS_COCA_BK

PE09(config-if)#ip vrf forwarding dat1010

PE09(config-if)#ip address 10.10.10.197 255.255.255.252

PE09(config-if)#no shutdown

3.3.3.2 CE

En la interface FastEthernet0/1 se configuró la IP del enlace backup para el enlace de datos.

URBANO_EXPRESS_COCA(config)#interface FastEthernet0/1

URBANO_EXPRESS_COCA(config-if)#description WAN_PNET_BK

URBANO_EXPRESS_COCA(config-if)#ip address 10.10.10.198 255.255.255.252

URBANO_EXPRESS_COCA(config-if)#no shutdown

Con estas configuraciones se obtuvo conectividad desde el PE backup hacia el CE y viceversa.

PE Backup hacia el CE

PE02#ping vrf dat1010 10.10.10.198
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.198, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CE hacia el PE Backup

URBANO_EXPRESS_COCA#ping vrf datos 10.10.10.197
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.197, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

3.3.4 Configuración del protocolo BGP

3.3.4.1 PE Backup

Se configuró en el PE backup dentro de las sesiones BGP y la VRF correspondiente del enlace de datos con las siguientes consideraciones.

El número de sistema autónomo local para el enlace de datos es el 56001 en la VRF dat1010 definida en la address family de ipv4, el sistema autónomo remoto es el 64514 más adelante configurará en el CE con el vecindad 10.10.10.198.

PE09(config)#router bgp 56001
PE09(config-router)address-family ipv4 vrf dat1010
PE09(config-router-af)#neighbor 10.10.10.198 remote-as 64514
PE09(config-router-af)#neighbor 10.10.10.198 description
URBANO_EXPRESS_BK
PE09(config-router-af)#neighbor 10.10.10.198 activate
PE09(config-router-af)#neighbor 10.10.10.198 as-override

3.3.4.2 CE

Para designar el enlace principal del backup a nivel de la última milla se configuraron políticas (route-map). Las política que se creó es para las subredes de entrada al CE, esta política tiene el nombre de entrada backup configurado un local-preference de 200.

URBANO_EXPRESS_COCA(config)#route-map entrada_bk permit 10
URBANO_EXPRESS_ COCA(config-route-map)#set local-preference 200
URBANO_EXPRESS_ COCA(config-route-map)#exit
URBANO_EXPRESS_ COCA(config)#route-map entrada_bk deny 20

Se creó una política de salida de las subredes del CE para el enlace backup de datos, esta política tiene el nombre de salida backup configurada con un path de cuatro sistemas autónomos.

URBANO_EXPRESS_COCA(config)#route-map salida_bk permit 10
URBANO_EXPRESS_COCA(config-route-map)#set as-path prepend 64514 64514 64514
URBANO_EXPRESS_COCA(config-route-map)#exit
URBANO_EXPRESS_COCA(config)#route-map salida_bk deny 20

Una vez creada las políticas se procedió a realizar las siguientes configuraciones: definir el sistema autónomo remoto que es el 56001 relacionado con su vecino, activar la vecindad del enlace backup, habilitar el allowas-in para llegar hacia las subredes matriz y resto de sucursales que tienen el mismo sistema autónomo, también se relaciona las políticas creadas de entrada y de salida con su respectivas vecindades.

URBANO_EXPRESS_COCA(config)#router bgp 64514
URBANO_EXPRESS_COCA(config-router)address-family ipv4
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.197 remote-as
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.197 description bk

URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.197 activate
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.197 allowas-in
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.197 route-map entrada_bk in
URBANO_EXPRESS_COCA(config-router-af)#neighbor 10.10.10.197 route-map salida_bk out

3.4 Configuración del Software de Monitoreo Observium

Cada uno de los enlaces que se migró a la red MPLS fue ingresado en el software de monitoreo Observium permitiendo mantener un monitoreo constante de cada uno de los enlaces a nivel nacional, todas las configuraciones se realizaron en modo consola del servidor pero su verificación es modo gráfico, amigable al usuario.

3.4.1 Configuración inicial del host

En la configuración global del servidor en el que se encuentra la aplicación del Observium, se ingresó mediante vim al archivo hosts ubicado en el directorio /etc/ como se indica a continuación:

[root@localhost ~]# vim /etc/hosts

En este archivo se introduce una línea con la IP WAN del router y el nombre del enlace, con esta información escrita salimos del archivo de configuración presionando la tecla ESC, seguida de las siguientes teclas (:wq), la tecla ESC cambia de modo escritura a modo lectura dentro del archivo y el wq permite salir guardando los cambios realizados en el archivo. La línea de comando se encuentra de la siguiente manera:

10.10.10.2 Urbano_Express_Matriz_Datos_principal

3.4.2 Configuración inicial para añadir un host

Pasamos al directorio /opt/observium para cambiar del directorio raíz al directorio del Observium es mediante cd, como se indica a continuación:

[root@localhost ~]# cd /opt/observium/
[root@localhost observium]#

Desde el directorio del Observium se añadió el enlace con su respectivo nombre, la comunidad de monitoreo y la versión del software como se indica en las siguientes líneas de configuración.

[root@localhost observium]# ./add_device.php
Urbano_Express_Matriz_Datos_principal tornado v2c
Trying v2c community tornado ...

Now discovering urbano_express_matriz_datos_principal (id = 309)
urbano_express_matriz_datos_principal 309 ios (cisco)
urbano_express_matriz_datos_principal 309 ios (cisco)
IPv4 Addresses : N+N+N++N+N+N+
Discovered in 0.605 seconds

urbano_express_matriz_datos_principal 309 ios (cisco)
IPv6 Addresses :
Discovered in 0.177 seconds

Added device urbano_express_matriz_datos_principal (309)
[root@localhost observium]#

3.4.3 Configuración inicial para descubrir el host

Una vez que se ingresó el nombre del enlace con su correspondiente IPv4 se procede a descubrir el host, en este proceso el software realiza un inventario general del router.

[root@localhost observium]# ./discovery.php -h
Urbano_Express_Matriz_Datos_principal
Observium v0.13.10.4585
Discovery
urbano_express_matriz_datos_principal 309 ios (cisco)
Ports : .....
Port Stack: ++++++++++++++++++++++++++++++

Physical Inventory :
Caching OIDs: entPhysicalEntry
entAliasMappingIdentifier++++++++++++++++++++++++++
Processors : CISCO-PROCESS-MIB: + hrDevice:
Memory : OLD-CISCO-MEMORY-POOL: ++ CISCO-ENHANCED-MEMORY-POOL: ++
IPv4 Addresses : .....
IPv6 Addresses :
Sensors: CISCO-ENTITY-SENSOR: Caching OIDs: entSensorType entSensorScale entSensorValue entSensorMeasuredEntity entSensorPrecision entSensorThresholdSeverity entSensorThresholdRelation entSensorThresholdValue ENTITY-SENSOR: Caching OIDs: entPhySensorType entPhySensorScale entPhySensorPrecision entPhySensorValue
CISCO-ENVMON-MIB Temp ciscoEnvMonTemperatureStatusDescr ciscoEnvMonTemperatureStatusValue
ciscoEnvMonTemperatureThreshold++++++ Volts
ciscoEnvMonVoltageStatusDescr ciscoEnvMonVoltageStatusValue ciscoEnvMonVoltageThresholdLow ciscoEnvMonVoltageThresholdHigh++++++++
Storage :
hrDevice :
Discovery protocols: CISCO-CDP-MIB: ++ LLDP-MIB:
OSPF Neighbours:
ARP/NDP Tables :
++
++
++++++++++++++++++++++++++++++++++
BGP Sessions: AS64514 Updated ASN (from -> 64514)
++++
VLANs:
Q-BRIDGE-MIB VLANs : VLAN version1
Cisco VLANs : VTP Domain 1 1+ 10+ 11+ 20+ 100+ 200+ 1002+ 1003+ 1004+ 1005+

VLAN 1

VLAN 10

dot1d id ifIndex Port Name Priority State Cost

4 9 FastEthernet0/0/3 128 forwarding 19 Inserted

VLAN 11

dot1d id ifIndex Port Name Priority State Cost

3 8 FastEthernet0/0/2 128 forwarding 19 Inserted

VLAN 20

dot1d id ifIndex Port Name Priority State Cost

2 7 FastEthernet0/0/1 128 forwarding 19 Inserted

VLAN 100

VLAN 200

Cisco Pseudowires :

VRFs :

SLAs :

Toner :

UCD Disk IO :

Discovered in 20.21 seconds

Current Revision : 4585

New Revision : 7133

MySQL: Cell[3/0s] Row[63/0.02s] Rows[18/0s] Column[1/0s] Update[2/0.23s] Insert[233/11.58s] Delete[0/0s]

[root@localhost observium]#

3.4.4 Configuración inicial para poller

Es el proceso final en el que el software Observium realiza un análisis detallado del router como interfaces físicas y virtuales, versión, direcciones IPv4, marca del roeuter, voltaje de funcionamiento y el protocolo por el cual esta realizando el enrutamiento del servicio.

[root@localhost observium]# ./poller.php -h Urbano_Express_Matriz_Datos_principal

Observium v0.13.10.4585

Poller

Starting polling run:

urbano_express_matriz_datos_principal 309 ios (cisco)
Created directory : /opt/observium/rrd/urbano_express_matriz_datos_principal
Module [unix-agent] disabled globally.
Using SNMP Agent sysUpTime (1997867 seconds)
Uptime: 23 days, 2h 57m 47s
Module time: 1.6028s
Hardware: cisco2921 Version: 15.4(1)T1 Features: UNIVERSALK9 Serial: Asset:
Module time: 0.1425sIPMI:
Module time: 0.0057sSensors:
Checking (snmp) temperature CPU 51 C

Checking alerts
Checking (snmp) temperature Intake Left 25 C

Checking alerts
Checking (snmp) temperature Intake Right 21 C

Checking alerts
Checking (snmp) temperature Exhaust Left 28 C

Checking alerts
Checking (snmp) temperature Exhaust Right 26 C

Checking alerts
Checking (snmp) temperature Power Supply 26 C

Checking alerts
Checking (snmp) voltage 12V voltage in mV 12782 V

Checking alerts
Checking (snmp) voltage 5V voltage in mV 5187 V
Checking alerts
Checking (snmp) voltage 3.3V voltage in mV 3335 V
Checking alerts
Checking (snmp) voltage 2.5V voltage in mV 2512 V
Checking alerts
Checking (snmp) voltage 1.8V voltage in mV 1830 V

Checking alerts
Checking (snmp) voltage 1.2V voltage in mV 1210 V

Checking alerts
Checking (snmp) voltage ASIC voltage in mV 1054 V

Checking alerts
Checking (snmp) voltage CPU Core voltage in mV 1220 V

Checking alerts
Module time: 0.8751sProcessor Processor 1 1%

Checking alerts
Module time: 0.0825sMempool Processor: 3.77%
Checking alerts

Mempool I/O: 45.48%
Checking alerts

Mempool CISCO2921/K9 - Processor: 3.77%
Checking alerts

Mempool CISCO2921/K9 - I/O: 45.48%
Checking alerts

Module time: 0.3367sModule time: 0.0007sPolling Netstats: IP TCP UDP ICMP SNMP
Module time: 0.8052sHR StatsModule time: 0.0133sModule time: 0.0459sPolling IP-MIB ipSystemStats ipv4 ipv6
Module time: 0.1817sCaching Oids: ifEntry ifXEntry dot3StatsDuplexStatus
Port Embedded-Service-Engine0/0(1) dot3Duplex, VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress ifPromiscuousMode ifConnectorPresent ifDuplex bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port GigabitEthernet0/0(2) replacing with 64-bit...dot3Duplex, VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress ifPromiscuousMode ifConnectorPresent ifDuplex bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port GigabitEthernet0/1(3) replacing with 64-bit...dot3Duplex, VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress ifPromiscuousMode ifConnectorPresent ifDuplex bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port GigabitEthernet0/2(4) replacing with 64-bit...dot3Duplex, VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress ifPromiscuousMode ifConnectorPresent ifDuplex bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port Backplane-GigabitEthernet0/3(5) replacing with 64-bit...VLAN ==
ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress
ifPromiscuousMode ifConnectorPresent
bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port FastEthernet0/0/0(6) replacing with 64-bit...dot3Duplex, VLAN ==
20ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress
ifPromiscuousMode ifConnectorPresent ifDuplex ifVlan
bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts
Port FastEthernet0/0/1(7) replacing with 64-bit...dot3Duplex, VLAN ==
20ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress
ifPromiscuousMode ifConnectorPresent ifDuplex ifVlan
bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port FastEthernet0/0/2(8) replacing with 64-bit...dot3Duplex, VLAN ==
11ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress
ifPromiscuousMode ifConnectorPresent ifDuplex ifVlan
bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port FastEthernet0/0/3(9) replacing with 64-bit...dot3Duplex, VLAN ==
10ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress
ifPromiscuousMode ifConnectorPresent ifDuplex ifVlan
bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port Null0(10) HighSpeed, VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed
ifHighSpeed ifPromiscuousMode ifConnectorPresent
bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)

Checking alerts

Port Vlan1(11) replacing with 64-bit...dot3Duplex, VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress ifPromiscuousMode ifConnectorPresent ifDuplex bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port GigabitEthernet0/2.3211(12) replacing with 64-bit...VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress ifPromiscuousMode ifConnectorPresent bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port GigabitEthernet0/2.3222(13) replacing with 64-bit...VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress ifPromiscuousMode ifConnectorPresent bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port Vlan10(14) replacing with 64-bit...dot3Duplex, VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress ifPromiscuousMode ifConnectorPresent ifDuplex bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port Vlan11(15) replacing with 64-bit...dot3Duplex, VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress ifPromiscuousMode ifConnectorPresent ifDuplex bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Port Vlan20(16) replacing with 64-bit...dot3Duplex, VLAN == ifAdminStatus ifOperStatus ifMtu ifSpeed ifHighSpeed ifPhysAddress ifPromiscuousMode ifConnectorPresent ifDuplex bps(0bps/0bps)bytes(0B/0B)pkts(0pps/0pps)
Checking alerts

Module time: 2.3809sBGP Peers: Caching: (CISCO-BGP4-MIB) cbgpPeer2State cbgpPeer2AdminStatus cbgpPeer2InUpdates cbgpPeer2OutUpdates cbgpPeer2InTotalMessages cbgpPeer2OutTotalMessages cbgpPeer2FsmEstablishedTime cbgpPeer2InUpdateElapsedTime cbgpPeer2LocalAddr cbgpPeer2RemoteIdentifier cbgpPeer2AcceptedPrefixes cbgpPeer2DeniedPrefixes cbgpPeer2PrefixAdminLimit cbgpPeer2PrefixThreshold cbgpPeer2PrefixClearThreshold cbgpPeer2AdvertisedPrefixes cbgpPeer2SuppressedPrefixes cbgpPeer2WithdrawnPrefixes Checking BGP peer: 10.10.10.1
Checking alerts

Checking BGP peer: 10.10.10.5
Checking alerts

Checking BGP peer: 192.168.43.37
Checking alerts

Checking BGP peer: 192.168.43.41
Checking alerts

Module time: 1.109sModule time: 0.0006sModule time: 0.0005sModule time: 0.0004sWireless:
Module time: 0.0002sOSPF: Processes: Areas: Ports: Neighbours:
Module time: 0.1391sModule time: 0.0345sModule time: 0.0158sCisco CEF Switching Path: Caching OIDs: entPhysicalDescr entPhysicalName entPhysicalModelName
Module time: 0.096sModule time: 0.0971sMac Accounting: Caching DB...0 entries. Cisco Entries:
-0-000000000000 + () -> 000000000000 1 MAC accounting entries

Module time: 0.1163sModule time: 0.0003sModule time: 0.0496s
Module time: 0.0307sModule time: 0.024sModule time: 0.0001sArray

Module time: 0.0197sModule time: 0.0005sModule time: 0.0002sEntity Physical: Cisco Cat6xxx/76xx Crossbar :
Module time: 0.0584sModule time: 0.0003sFDB Tables
Vlan | MAC | Port (dot1d|ifIndex) | Status

Module time: 0.0009s+ping +ping_snmp +uptime +processor +mempool +netstat_ip +netstat_ip_frag +netstat_tcp +netstat_udp +netstat_icmp +netstat_icmp_info +netstat_snmp +netstat_snmp_pkt +ipsystemstats_ipv4 +ipsystemstats_ipv4_frag +ipsystemstats_ipv6 +ipsystemstats_ipv6_frag +poller_perf Polled in 9.0063 seconds
UPDATED!
MySQL: Cell[1/0s] Row[10/0s] Rows[37/0.01s] Column[0/0s] Update[65/0.74s] Insert[61/0.99s] Delete[0/0s]
[root@localhost observium]#

3.4.5 Crear usuario monitoreo

Se crea un usuario para que el cliente pueda monitorear cada uno de sus enlaces y también visualice el consumo del ancho de banda de cada uno de estos. El usuario que se crea se asigna un nombre, contraseña y el privilegio que este tiene en este caso es uno el cual es de lectura.

[root@localhost observium]# ./adduser.php UrbanoExpress urbano2015express 1
User UrbanoExpress added successfully.
[root@localhost observium]#

4. Capítulo IV. Ejecución y Resultados

4.1 Pruebas de funcionamiento de la red

Cada sucursal que se migró a la red MPLS se realizó pruebas de conectividad y funcionamiento de todas las aplicaciones de la empresa Urbano Express.

4.1.1 Pruebas de conectividad

Las pruebas de conectividad se realizó mediante un ping y tracert, también se verificó que las aplicaciones estén funcionando correctamente por parte del cliente.

En la ciudad de Quito se encuentran los servidores de aplicaciones más importantes y críticos que diariamente utilizan los usuarios a nivel nacional, por tal motivo, cada sucursal que se migró a la nueva red MPLS se realizó pruebas de comunicación a la LAN de matriz Quito y a la WAN, es decir, desde el PE hasta el CE y viceversa.

La primera prueba de conectividad de la WAN se realiza desde el PE principal hasta el CE, en el ping se especifica la VRF y también el número de repetición de 1000.

PE02#ping vrf dat1010 10.10.10.2 repeat 1000

Type escape sequence to abort.

Sending 1000, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

!!
!!
!!
!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/2/80 ms

Se evidencia que no existen paquetes perdidos entre la comunicación del PE y CE se tiene un 100 % de paquetes recibidos comprobando que la última milla está correcta, los tiempos de respuesta promedio son de 2 milisegundos que está en el rango de tecnología de fibra óptica, de similar forma se realizó con el enlace de backup entre el PE backup y CE.

PE03#ping vrf dat1010 10.10.10.6 repeat 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 10.10.10.6, timeout is 2 seconds:
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/2/94 ms

Una vez que la última milla está correcta se verificó la comunicación mediante un ping desde la LAN de la sucursal hasta la LAN de matriz en Quito, en el paquete icmp se especificó la VRF de datos, la IP destino 192.168.18.200, la IP origen 192.168.1.7 y una repetición de 500.

URBANO_*EXPRESS_DATOS_INTERNET_MATRIZ#*
ping vrf datos 192.168.18.200 source 192.168.1.7 repeat 500
Type escape sequence to abort.
Sending 500, 100-byte ICMP Echos to 192.168.18.200, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.7
!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 4/6/16 ms

Con las verificaciones anteriores se garantiza la comunicación de extremo a extremo con tiempos de respuesta adecuados y sin perdidas de paquetes en la conexión, además se realizó pruebas de acceso a internet de la sucursal.

URBANO_EXPRESS_COCA#ping 8.8.8.8 source 192.168.18.200 repeat 500
Type escape sequence to abort.
Sending 500, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.18.200
!!
!!
!!
!!
!!

!!
!!
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 64/69/164 ms

El resultado del comando indica que no existe paquetes perdidos y un tiempo promedio de 69 milisegundos a los DNS de google 8.8.8.8.

Con un tracert constamos el acceso al internet sea por la mejor métrica, que es el enlace principal del concentrador Quito, el tracert está constituido con la IP destino 8.8.8.8 DNS google y la IP origen la 192.168.18.200.

URBANO_EXPRESS_COCA#traceroute 8.8.8.8 source 192.168.18.200
Type escape sequence to abort.
Tracing the route to 8.8.8.8
1 10.10.10.193 12 msec 12 msec 4 msec
2 10.10.10.1 [AS 56001] 8 msec 4 msec 16 msec
3 10.10.10.2 [AS 56001] 8 msec 4 msec 8 msec
4 20.20.20.2 [AS 56001] 8 msec 8 msec 8 msec
5 181.49.11.1 [AS 56001] 4 msec 8 msec 8 msec
6 192.168.43.41 [AS 56001] 12 msec 24 msec 12 msec
*190.90.102.33 [AS 65001] 76 msec 56 msec 10 * **
213.140.51.219 [AS 65001] 24 msec
7 209.85.241.101 [AS 65001] 72 msec
209.85.253.79 [AS 65001] 64 msec
209.85.252.93 [AS 65001] 84 msec
8 8.8.8.8 [AS 65001] 68 msec

En el tracert se evidencia que las peticiones para acceso al internet están realizando por el enlace principal de matriz Quito debido que en el salto indica la 10.10.10.2 que pertenece a la IP del enlace principal de Matriz Quito.

4.1.2 Pruebas de ancho de banda

En el concentrador de matriz Quito para el enlace de acceso a internet principal y backup se tiene un ancho de banda de 45 Mbps simétricos y dedicados.

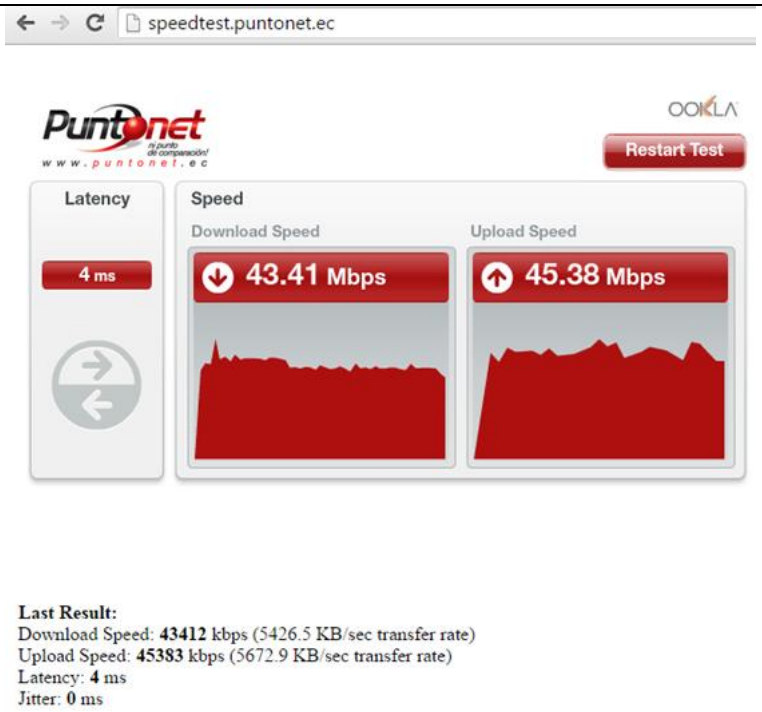

Figura 56. Ancho de banda de acceso a internet matriz Quito

En la figura 55 se evidencia el test de velocidad del enlace de matriz Quito, este test se realizó en la página wed con URL speedtest.puntonet.ec.

El enlace de datos en matriz no se puede medir con un test de velocidad, por tal motivo, se emplea un server ftp para poder realizar una carga y descarga desde un usuario final con filezilla.

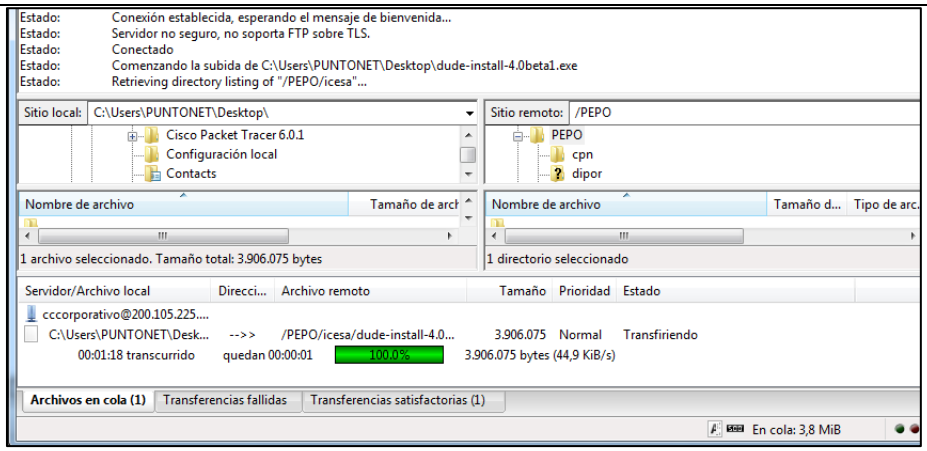

Figura 57. Transferencia de información server FTP

Los enlaces de datos de las sucursales a nivel nacional tienen un ancho de banda de 1.5 Mbps como estos enlaces tienen acceso a internet desde matriz se puede medir la capacidad con un test o ftp.

4.1.3 Pruebas de MTU

El MTU es uno de los parámetros técnicos más importantes de una conexión, por tal motivo, en cada uno de los enlaces se probó un MTU mínimo de 1500, con este valor garantizamos que cualquier aplicación que Urbano Express necesite funcione correctamente.

Se garantizó un MTU mínimo de 1500 extremo a extremo, es decir, desde la LAN de matriz Quito hasta la LAN de la sucursal, en este ping se especifica la VRF, IP destino, IP origen, el tamaño del paquetes de 1500 y 500 repeticiones.

URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#ping vrf datos 192.168.18.200 source 192.168.1.7 size 1500 repeat 500

Type escape sequence to abort.

Sending 500, 1500-byte ICMP Echos to 192.168.18.200, timeout is 2 seconds:

Packet sent with a source address of 192.168.1.7

!!!

!!!

!!!

!!

!!

!!

!!

!!!!!!!!!!

Success rate is 100 percent (500/500), round-trip min/avg/max = 4/9/72 ms

De similar forma se verificó paquetes con MTU mayor a 1500, en este caso se probó con un MTU de 2000.

URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#ping vrf datos 192.168.18.200 source 192.168.1.7 size 2000 repeat 500

Type escape sequence to abort.

Sending 500, 2000-byte ICMP Echos to 192.168.18.200, timeout is 2 seconds:

Packet sent with a source address of 192.168.1.7

!!

!!

!!

!!

!!

!!

!!

!!!!!!!!!!

Success rate is 100 percent (500/500), round-trip min/avg/max = 4/9/32 ms

También se tiene que realizar una verificación de MTU desde la sucursal hasta la matriz datos quito, este ping tiene similar valores que el de matriz como IP destino, IP origen, tamaño del paquete y número de repeticiones.

URBANO_EXPRESS_COCA#ping 192.168.1.7 source 192.168.18.200 size 1500 repeat 500

Type escape sequence to abort.

Sending 500, 1500-byte ICMP Echos to 192.168.1.7, timeout is 2 seconds:

Packet sent with a source address of 192.168.18.200

!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 4/9/64 ms

4.1.4 Pruebas de conmutación automática BK

Todos los enlaces cuentan con backup a nivel de la última milla, para que este backup sea eficiente tiene que conmutar de manera automática y con un tiempo mínimo de afectación a las operaciones diarias, el protocolo BGP empleado para seleccionar entre principal y backup.

Con el comando show ip bgp summary se verificó que la sesión BGP de las dos vecindades estén establecidas, en este caso se realizó la consulta del servicio de datos con la VRF datos.

URBANO_EXPRESS_GYE_DATOS_INTERNET#sh ip bgp vpnv4 vrf datos summary

```
Neighbor V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.9      4 56001  125401  108542     2270    0    0 5d01h         45
10.10.10.13     4 56001  127523  107105     2270    0    0 5d16h         46
```

Para verificar que el servicio este funcionado correctamente por el enlace principal, se realizó una consulta a una subred LAN de Quito mediante el comando show ip route especificando la VRF de datos como se indica a continuación:

URBANO_EXPRESS_GYE_DATOS_INTERNET#sh ip route vrf datos 192.168.1.4

Routing entry for 192.168.1.0/24

Known via "bgp 64514", distance 20, metric 0
Tag 56001, type external
Last update from 10.10.10.9 5d01h ago
Routing Descriptor Blocks:
** 10.10.10.9, from 10.10.0.9, 5d01h ago*
Route metric is 0, traffic share count is 1
AS Hops 2
Route tag 56001

Para verificar que la conmutación funcione correctamente se procedió a bajar la interface VLAN del enlace principal en el PE.

interface Vlan2909
description URBANO_EXPRESS_PRINCIPAL_DATOS
ip vrf forwarding dat1010
ip address 10.10.10.9 255.255.255.252
shutdown
end

Una vez la interfaz VLAN que se encuentre administrativamente down no se puede llegar a la IP 10.10.10.9 desde el propio PE.

PE10#ping vrf dat1239 10.10.10.9
% VRF dat1239 does not have a usable source address

Se verificó que desde el CE no se tiene conectividad a la WAN del enlace que tiene la IP 10.10.10.9 con la VRF datos.

URBANO_EXPRESS_GYE_DATOS_INTERNET#ping vrf datos 10.10.10.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.9, timeout is 2 seconds:
.....

Success rate is 0 percent (0/5)

En las sesiones BGP del CE se verifica que la vecindad del enlace principal no está establecida pero la del enlace backup si está funcionando.

URBANO_EXPRESS_GYE_DATOS_INTERNET#sh ip bgp vpnv4 vrf datos summary

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.9 4 56001 125472 108589 0 0 0 00:00:21 Active
10.10.10.13 4 56001 127573 107156 2448 0 0 5d17h 44

Para verificar que el servicio este funcionado correctamente por el enlace backup, se realizó una consulta a una subred LAN de Quito mediante el comando show ip route especificando la VRF de datos como se indica a continuación:

URBANO_EXPRESS_GYE_DATOS_INTERNET#sh ip route vrf datos 192.168.1.0

Routing entry for 192.168.1.0/24
Known via "bgp 64514", distance 20, metric 0
Tag 56001, type external
Last update from 10.10.10.13 00:01:21 ago
Routing Descriptor Blocks:
** 10.10.10.13, from 10.10.10.13, 00:01:21 ago*
Route metric is 0, traffic share count is 1
AS Hops 2
Route tag 56001

Se evidencia que para llegar a la subred de matriz Quito está saliendo por el enlace de backup que tiene la IP WAN 10.10.10.13.

También se realizó las pruebas de acceso a internet mediante el concentrador de Guayaquil, en el traceroute se puede evidenciar que el acceso al internet es por la red de Guayaquil 10.10.10.10.

URBANO_EXPRESS_COCA#traceroute 8.8.8.8 source 192.168.18.200

Type escape sequence to abort.

Tracing the route to 8.8.8.8

1 10.10.10.193 4 msec 16 msec 8 msec

2 10.10.10.9 [AS 65001] 12 msec 20 msec 8 msec

3 10.10.10.10 [AS 65001] 16 msec 12 msec 20 msec

4 30.30.30.2 [AS 65001] 24 msec 12 msec 12 msec

5 190.12.0.205 [AS 65001] 12 msec 8 msec 16 msec

6 192.168.217.197 [AS 65001] 16 msec 16 msec 12 msec

7 192.168.173.5 [AS 65001] 12 msec 12 msec 12 msec

8 201.234.219.89 [AS 65001] 12 msec 60 msec 12 msec

9 67.16.166.57 [AS 65001] 104 msec 92 msec 92 msec

10 67.16.147.142 [AS 65001] 108 msec 104 msec 108 msec

11 72.14.210.75 [AS 65001] 96 msec

72.14.210.73 [AS 65001] 100 msec

74.125.48.93 [AS 65001] 100 msec

12 216.239.50.55 [AS 65001] 88 msec

216.239.50.67 [AS 65001] 116 msec

216.239.50.59 [AS 65001] 96 msec

13 216.239.51.143 [AS 65001] 112 msec

216.239.50.119 [AS 65001] 104 msec

216.239.50.117 [AS 65001] 96 msec

14 8.8.8.8 [AS 65001] 92 msec 104 msec 104 msec

4.2 Análisis Técnico y Económico

4.2.1 Análisis técnico de convergencia de la red

Todos los puntos a nivel nacional han sido migrado satisfactoriamente a la red MPLS, en la actualidad todos los enlaces cuenta con dos últimas millas, un router, el protocolo de enrutamiento dinámica BGP y una topología estándar para todas las sucursales facilitando el soporte técnico de primer nivel por parte del personal de Puntonet.

A demás se implementó el software de monitoreo para todos los enlaces a nivel nacional, con este monitoreo se brindará un soporte proactivo por parte de Puntonet a Urbano Express y también se podrá verificar el consumo de ancho de banda de los diferentes canales.

La última milla es primordial para prestar una alta disponibilidada en los servicios prestados, por tal motivo, en la mayoría de los puntos se implementó fibra óptica en los enlaces principales, debido que, la latencia es de 1 a 2 milisegundos y soporta anchos de banda mayor comparado con los radio enlaces, ADSL o VSAT. Los enlaces de backup se implementó la última milla de radio enlace que tiene una latencia alrededor de 20 milisegundos pero su funcionamiento depende mucho de las condiciones ambientales como: frecuencia y distancia entre la radio base y radio remota, también en lugares donde se presenta restricciones geográficas se implementó como última milla ADSL o VSAT, con las dos últimas millas implementadas de diferente tecnología se garantiza una alta redundancia con un uptime del servicio del 99.99 %.

Los routers implementados son de marca Cisco y Mikrotik por ser robustos frente a diferentes condiciones ambientales, cuenta con diferentes interfaces y soporta protocolo de enrutamiento dinámico como BGP, por tal motivo, fueron idóneos para la implementación en la red MPLS.

El protocolo BGP es el más estable que se puede emplear en la actualidad por sus métrica que facilitan la conmutación automática de los enlaces principal y backup, además de ser un protocolo escalable que facilita aumentar de nuevos sucursales a nivel nacional. La disponibilidad de cada uno de los enlaces es alta, por la topología implementada, la red de transporte MPLS y por el protocolo de enrutamiento BGP, con sus ventajas, BGP asegura la fiabilidad del transporte llevando sus actualizaciones de routing y sincronizando las actualizaciones, soporta VLSM, sumarización, IPv4, e IPv6.

Con la nueva topología implementada todas los enlaces tienen la misma métrica, es decir, para llegar de una sucursal a matriz o a otra sucursal se ve como un enlace punto a punto dentro de la red MPLS, optimizando los tiempos de

respuesta debido que el número de saltos dentro de la red es menor, también garantizando un MTU de 1500 de extremo a extremo y calidad de servicio en toda la red de transporte de MPLS, otro aspecto muy importante a considerar es que se tiene un red totalmente escalable y fullmesh.

La tabla de enrutamiento en cada uno de los routers técnicamente es fácil de interpretar por estar enrutadas dinámicamente, dedio que el router CE anuncia sus subredes al PE y este a su vez al resto de PEs a nivel nacional garantizando una comunicación optima y eficiente.

A continuación, se indica la tabla de enrutamiento de matriz.

URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#sh ip route vrf datos

Routing Table: datos
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override

Gateway of last resort is 10.10.10.1 to network 0.0.0.0

B 0.0.0.0/0 [20/0] via 10.10.10.1, 19:25:16*
10.0.0.0/8 is variably subnetted, 59 subnets, 2 masks
S 10.0.0.0/30 [1/0] via 192.168.1.82
S 10.0.5.0/30 [1/0] via 192.168.1.82
S 10.0.6.0/30 [1/0] via 192.168.1.82
C 10.10.10.0/30 is directly connected, GigabitEthernet0/0

L 10.10.10.2/32 is directly connected, GigabitEthernet0/0
B 10.10.10.4/30 [20/0] via 10.10.10.1, 09:40:10
B 10.10.10.8/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.12/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.16/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.20/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.24/30 [20/0] via 10.10.10.1, 17:34:12
B 10.10.10.28/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.32/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.36/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.40/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.44/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.48/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.52/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.56/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.60/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.64/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.68/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.72/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.76/30 [20/0] via 10.10.10.1, 09:40:10
B 10.10.10.80/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.88/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.92/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.104/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.112/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.116/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.120/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.124/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.128/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.132/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.144/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.148/30 [20/0] via 10.10.10.1, 19:25:16

B 10.10.10.152/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.156/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.160/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.164/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.168/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.176/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.180/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.184/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.188/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.192/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.200/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.208/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.216/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.224/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.228/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.240/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.10.248/30 [20/0] via 10.10.10.1, 19:25:16
B 1 0.1.240.16/30 [20/0] via 10.10.10.1, 19:25:16
B 10.1.240.24/30 [20/0] via 10.10.10.1, 19:25:16
B 10.1.240.32/30 [20/0] via 10.10.10.1, 19:25:16
B 10.1.240.40/30 [20/0] via 10.10.10.1, 19:25:16
B 10.1.240.44/30 [20/0] via 10.10.10.1, 19:25:16
B 10.10.170.0/30 [20/0] via 10.10.10.1, 09:40:10
172.16.0.0/24 is subnetted, 1 subnets
S 172.16.1.0 [1/0] via 192.168.1.82
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Vlan20
L 192.168.1.7/32 is directly connected, Vlan20
S 192.168.2.0/24 [1/0] via 192.168.1.82
B 192.168.3.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.4.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.5.0/24 [20/0] via 10.10.10.1, 19:25:16

B 192.168.7.0/24 [20/0] via 10.10.10.1, 02:03:57
B 192.168.9.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.10.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.11.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.12.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.13.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.15.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.16.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.17.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.18.0/24 [20/0] via 10.10.10.1, 19:20:39
B 192.168.19.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.20.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.21.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.22.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.23.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.24.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.25.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.27.0/24 [20/0] via 10.10.10.1, 04:24:00
B 192.168.28.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.29.0/24 [20/0] via 10.10.10.1, 17:34:12
B 192.168.30.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.31.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.33.0/24 [20/0] via 10.10.10.1, 19:25:16
B 192.168.39.0/24 [20/0] via 10.10.10.1, 19:25:16
S 192.168.41.0/24 [1/0] via 192.168.1.82
S 192.168.42.0/24 [1/0] via 192.168.1.82
B 192.168.51.0/24 [20/0] via 10.10.10.1, 05:55:15
B 192.168.53.0/24 [20/0] via 10.10.10.1, 19:25:16
197.1.2.0/25 is subnetted, 1 subnets
S 197.1.2.0 [1/0] via 192.168.1.4

Se puede evidenciar que todas las subredes externas, es decir las LANs de las sucursales y ruta por defecto aprende por la WAN principal que es la IPv4 10.10.10.1 de esta manera garantizando la comunicación con todos los enlaces a nivel nacional, cabe mencionar que es una parte de la tabla de enrutamiento.

Ademas todos los enlaces se tiene en el software de monitoreo Observium.

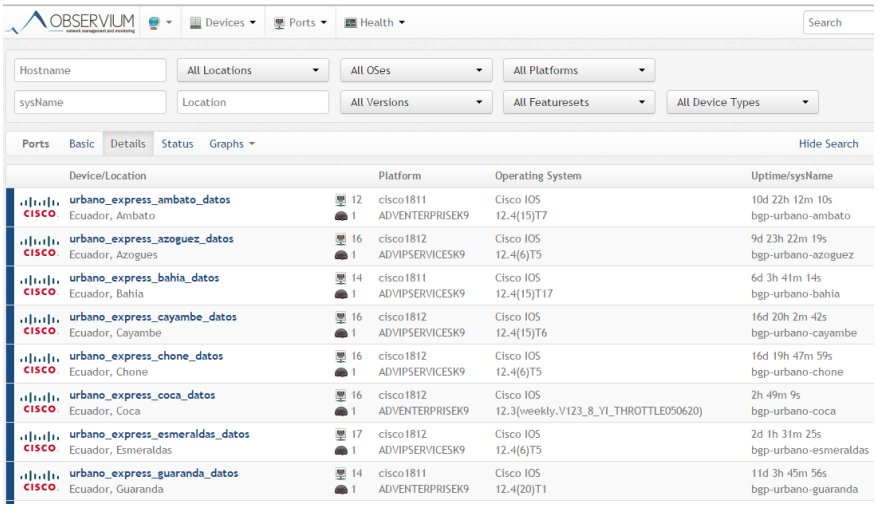

Figura 58. Enlaces en el Observium

En este software podemos verificar el historial del consumo del ancho de banda del enlace tanto de subida como de bajada.

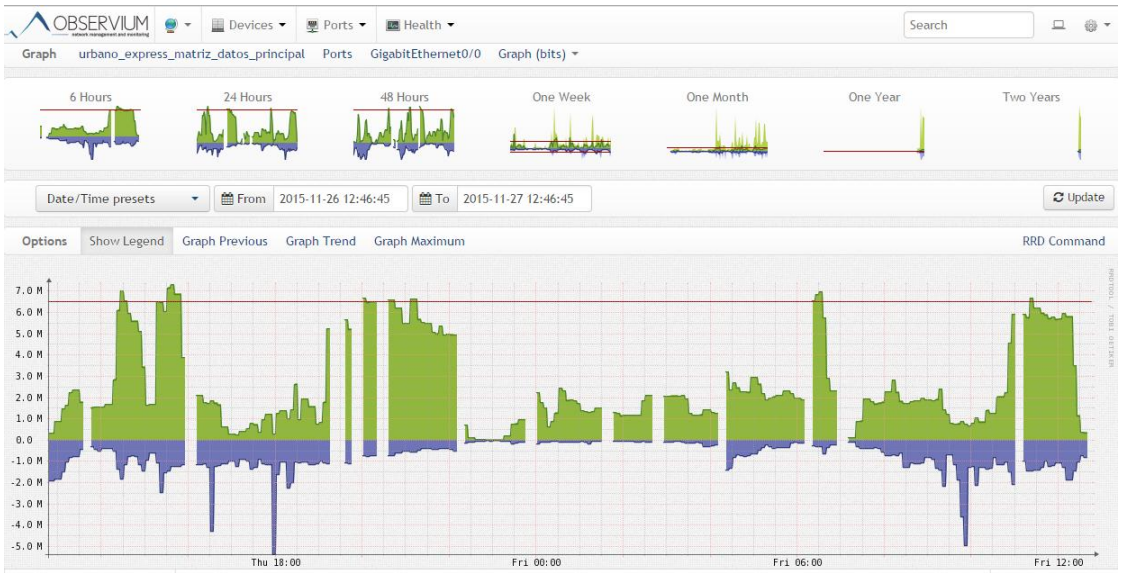

Figura 59. Consumo del enlace de matriz Quito

En el Observium se puede verificar algunos parámetros del router como memoria procesador, logs, tipo de enrutamiento y los puertos en los cuales se encuentra configurado.

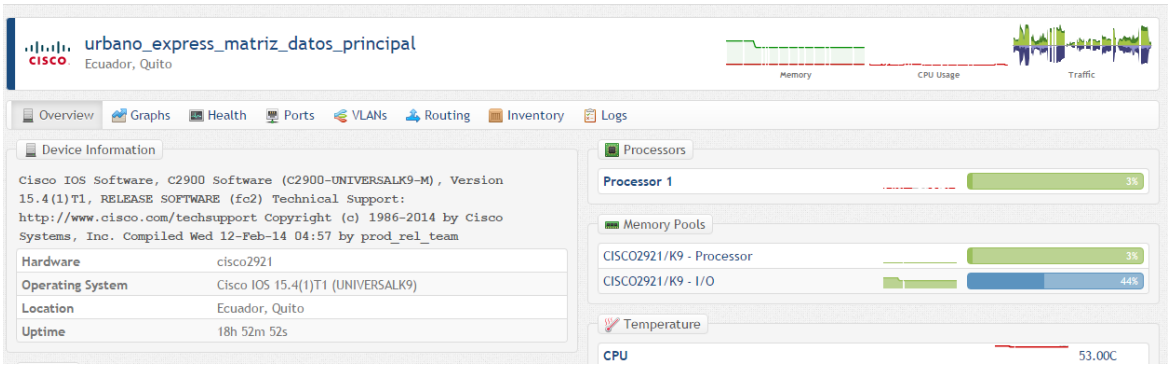

Figura 60. Estados del router cisco de matriz

4.2.2 Análisis económico costo / beneficio

A continuación, se presentará un análisis de los costos y beneficios asociados al proyecto.

En el análisis de costo se tomará como referencia la metodología del costo total de propiedad (TCO), con el cuál, mejorará el proceso de adquisición de tecnologías y costos asociados a estos identificando el valor económico de la inversión, para esta metodología se emplea los costos directos y los costos indirectos.

En el análisis de costos del proyecto se tiene tres componentes escenciales como son: técnico, profesionales y mantenimiento, para este proyecto en la parte técnica se mencionará el hardware y software de los servicios prestados, en el componente profesional se tomarán encuenta capacitaciones y consultorias, por último, el componente de mantenimiento reflejado en visitas técnicas.

Costos Directos

- **Técnicos**

En los costos técnicos directos se utilizó varios componentes como hardware (routers de marca Cisco y Mikrotik, ONT's de marca Corecess y Calix, antenas

de radio enlace de marca Metal), elementos de comunicación (patchcore de fibra y cobre), software (Observium), migración de tecnología (tiempo de desconexión) y otros costos (energía).

Tabla 5. Costos directos técnicos

Concepto	Cantidad	Valor	Total
Router Cisco 2921	1	$ 1.200,00	$ 1.200,00
Router Cisco 2811	1	$ 350,00	$ 350,00
Router Cisco 1811	17	$ 250,00	$ 4.250,00
Router Cisco 1812	16	$ 250,00	$ 4.000,00
Router Cisco 1841	2	$ 260,00	$ 520,00
Router Mikrotik 750	3	$ 65,00	$ 195,00
Router Mikrotik 2011	1	$ 110,00	$ 110,00
ONT Corecess	15	$ 82,00	$ 1.230,00
Antena Metal	8	$ 83,00	$ 664,00
Tranceiver	2	$ 380,00	$ 760,00
ONT Calix	6	$ 120,00	$ 720,00
Patch fibra	21	$ 5,40	$ 113,40
Patch cobre	100	$ 2,80	$ 280,00
Observium	1	$ -	$ -
Otros			$ 1.000,00
Total			$ 15.392,40

- **Profesionales**

  En los costos profesionales directos se consideró el salario del Account Mananger encargado de las migraciones al igual que la difusión y comunicación.

Tabla 6. Costos directos profesionales

Concepto	Total
Account Manager	$ 820,00

- **Mantenimiento**

  En los costos de mantenimiento directos se consideró el salario de los técnicos que se dirigieron a cada uno de los enlaces al momento de la migración.

Tabla 7. Costos directos de mantenimiento

Costo	Total
Técnico Sucursales	$ 750,00
Técnico de Radio	$ 500,00
Técnico Corporativo	$ 700,00
Total	$ 1.950,00

Costos Indirectos

En los costos indirectos también se encuentran inmersos los componentes técnicos, profesionales y de mantenimiento como por ejemplo el costo de la infraestructura de enlaces backup al igual que el tiempo implementado en el mismo, capacitación al personal de Call Center para el soporte respectivo y el costo de las horas de investigación dedicada a practicas o entrenamiento para solucionar problemas que se fueron presentando en el proyecto.

Tabla 8. Costos Indirectos

Concepto	Cantidad	Valor	Total
Enlaces Backup	38	$ 50,00	$ 1.900,00
Capacitación		$ 820,00	$ 820,00
Total			$ 2.720,00

En la tabla 9 se verifica los costos que invirtió el ISP Puntonet para migrar a la red MPLS de su cliente Urbano Express.

Tabla 9. Costos totales

Costos	Valos
Costos Directo Técnico	$ 15.932,40
Costos directo profesional	$ 820,00
Costos directo mantemiento	$ 1.950,00
Costos indirecto	$ 2.720,00
Total	$ 21.422,40

El análisis de los beneficios del proyecto se identifican dos beneficiaros como sonel ISP Puntonet y el usuario Urbano Express.

Beneficios para Urbano Express

El tiempo y los gastos son los principales beneficios que adoptó la empresa Urbano Express al estar en una red MPLS con enlaces de backup, esto debido, a que cada una de las sucursales y matriz tiene redundancia a nivel de la ultima milla garantizando un uptime un 99,99% de los servicios y también garantizando que cada una de las aplicaciones funcionen al 100%, evitando cualquier tipo de perdidas en su core de negocio por problemas de comunicación, el funcionamiento de las diversas aplicaciones se consigue técnicamente con un MTU minimo de 1500 en todos los enlaces.

Otro beneficio que podríamos mencionar es la transparencia de los servicios de datos y acceso a internet percibidos por el usuario, también la accesibilidad y usabilidad del software Observium que permite monitorear a cada uno de los enlaces a nivel nacional, en este monitoreo también se incluye consumo de ancho de banda, reportes de disponibilidad, estatus del equipo, etc. Todos los parámetros anteriormente mencionados son de gran utilidad al momento de la verificacion del SLA (véase anexo 1) contratato con el ISP.

Beneficios para Puntonet

Puntonet ofrece tecnologías de última generación que permiten una amplia interoperabilidad y compatibilidad, garantizando altos niveles de tráfico de datos y contenidos multimedia de manera confiable y segura. Con el cual, se beneficiara la empresa Urbano Express a nivel nacional mediante la nueva tecnología MPLS, así, obtendrá mejores beneficios en el servicio a nivel de flexibilidad, escalabilidad, tiempo, soporte y costos. Para adaptarse a los esquemas de tráfico que demanda el crecimiento tecnológico, ofreciendo servicios MPLS en capa 2 y en capa 3, otro beneficio que proporciona Puntonet S.A. es el monitoreo constante mediante un software especializado para administración, monitoreo de equipos y canales de conexión, mediante esto garantizar la calidad de los enlaces proporcionados al cliente.

El principal beneficio es la reducción de gastos en la operatividad de la red de Urbano Express, esto debido que los enlaces de datos utilizan la infraestructura

propia del ISP Puntonet y solo contara con dos accesos a internet a nivel nacional permitiendo la eliminación del uso de IP’s públicas en todas las sucursales, también se minimizó los costos en equipos terminales al reducir el uso de los routers a uno solo.

La disminución de tiempo en el momento de prestar el soporte de primer nivel por parte del personal de Puntonet, esto debido, a que cada uno de los enlaces cuenta con una ingeniería o topología similar y fácil de interpretar. El software de monitoreo Observium permitirá brindar un soporte proactivo, con esto minimizando los tiempos de indisponibilidad por parte del proveedor cumpliendo el SLA, así, evitando multas económicas y fomentando una buena reputación como ISP a nivel nacional.

5. Capítulo V Conclusiones y Recomendaciones

5.1 Conclusiones

- Todos los enlaces a nivel nacional de la Empresa Urbano Express en la actualidad han migrado y están en la red de transporte MPLS del ISP Puntonet S.A, la ingeniería o topología es similar y sencilla de ser interpretada, facilitando L gestión por parte del personal de Puntonet el momento que se llega a presentar un inconveniente.
- La red Metro Ethernet ha sido formidable por sus diferentes beneficios, cabe recalcar, que para la transmisión de datos en la actualidad se necesita una red más eficiente, con mayores velocidades, mayor ancho de banda, escalabilidad, fiabilidad, menor costos, conectividad full mesh, arquitectura sencillas, VPN, mayor uso de aplicaciones, implementar QoS, etc., todos estos requerimientos nos proporciona la red de transporte MPLS, por tal motivo, se procedio a realizar este proyecto.
- Para brindar los servicios de datos y acceso a internet de una manera segura, no compleja y de bajos costos se implemento el método de VRF LITE en cada uno de los routers de matriz, esto debido que VRF LITE crea diferentes tablas de enrutamiento virtuales en un router y aisla cada uno de los servicios de datos y acceso a internet, pese que fisicamente se encuentren en el mismo router.
- En las sucursales y matriz se implementó el protocolo de enrutamiento dinámico BGP para la comunicación entre el CE y PE, es decir, es un EBGP debido que el PE tiene un sistema automono diferente al CE, todos los enlaces cuentan con servicios de datos y acceso a internet empleando la misma última milla principal y backup, el backup es pasivo y entrará en funcionamiento de manera automático al momento que el principal presente alguna falla, con las métricas de BGP como el as-path y el local_preferens permite priorizar a las rutas de entrada y salida del CE hacia el PE designando entre enlaces principal y backup.

- Las subredes LAN de matriz y sucursales son difundidos por el CE hacia el PE y el PE hacia el resto de PEs a nivel nacional dentro de la red de transporte MPLS como prefijos mediante el protocolodo de enrutamiento BGP de una manera eficiente, eficaz, óptima, segura, etc.
- El software especializado Observium permite la administración, monitoreo de equipos, canales de conexión, verificar consumo de ancho de banda, obtener reportes de disponibilidad, logs de eventos, direccionamiento, estado de temperatura, memoria, procesamiento y localización del router, permitiendo brindar un soporte proactivo de los servicios prestados, también con la ventaja que es un software que no necesita licencia para su funcionamiento por ser open source y además cuenta con una interfaz amigable con el usuario final.
- La empresa Urbano Express en la actualidad cuenta con una red convergente de alta calidad permitiendo el funcionamiento de todas sus aplicaciones como datos, acceso a internet y VoIP, sin representar algún costo económico de su parte. El ISP Puntonet S.A con los servicios prestados representa un ahorro económico significativo al no utilizar IPs públicas y emplear un solo router en cada uno de los enlaces, otro aspecto a considerar, es que con la nueva red implementada reduce el costo de mantenimiento de la red por visitas frecuentes que se tenia que realizar anteriormente y el tiempo del Account Manager encargado de la cuenta de Urbano Express.
- En la nueva red implementada toda la información técnica y comercial se encuentra totalmente organizada, el funcionamiento de cada uno de los servicios datos y acceso a internet operaran al cien por ciento con una efectividad y redundancia total, minimizando costos de operación de la red y garantizando un excelente servicio al cliente Urbano Express, la red MPLS esta totalmente convergente, conectividad full mesh, rindiendo anchos de banda y velocidad conforme a lo contratado en cada enlace.

5.2 Recomendaciones

- Se debe instalar un router en paralelo en matriz para no perder la comunicación con el resto de sucursales, al momento que se realice la migración de cada sucursal, de esta manera, es transparente para cada enlace la migración con un tiempo de afectación minimo.
- Antes de la migración se debe realizar un análisis minucioso de todas las apliaciones que el usuario final emplea diariamente, para cuando se encuentre migrado a la nueva red se pueda verificar el funcionamiento correcto de las mismas aplicaciones, de similar formar verificar conectividad desde el router a los servidores críticos del core de nogocio.
- Utilizar el software de monitoreo Observium por parte Urbano Express y Puntonet S.A para brindar un soporte proactivo a todos los enlaces a nivel nacional.
- Migrar e implementar el mismo esquema por parte de Puntonet S.A a todas las empresas a las que provee los servicios de datos y acceso a internet a nivel nacional.
- Se recomienda que todas los ISPs implementen una red MPLS para sus clientes fines, de esta manera brindar un servicio óptimo reduciendo los costos de operación y los recursos que emplean diariamente en dar un servicio de las mis características.

REFERENCIAS

Itlalaguna (s.f.). Fibra Óptica. Recuperado el 20 de Octubre de 2015, de http://www.itlalaguna.edu.mx/Academico/Carreras/electronica/opteca/OPTOPDF7_archivos/UNIDAD7TEMA2.PDF

Radiocomunicaciones (s.f.). Radio enlace. Recuperado el 22 de Octubre de 2015, de http://www.radiocomunicaciones.net/radio-enlaces.html

Vsat (s.f.). Conceptos Satelital. Recuperado el 23 de Octubre de 2015, de http://www.vsat-systems.com/teleport-and-NOC/idirect/benefits/

Datateca (s.f.). ATM. Recuperado el 25 de Octubre de 2015, de http://datateca.unad.edu.co/contenidos/208053/2015_2/Unidad_3_Lecturas/Unidad%203/FrameRelay%20y%20ATM.pdf

Cisco.com. (s.f.). Conceptos MPLS. Recuperado el 2 de Septiembre de 2015, de http://www.cisco.com/web/strategy/docs/gov/IntegNet_Feb17_915_Lynn.pdf

tools.cisco. (s.f). Funcionamiento MPLS Recuperado el 2 de Septiembre de 2015, de http://tools.cisco.com/search/results/en/us/get#q=MPLS

Cioperu.pe. (s.f). Conceptos Observium. Recuperado el 3 de Septiembre de 2015, de http://cioperu.pe/articulo/17462/7-herramientas-gratuitas-que-toda-red-necesita/

Salazar, L. (s.f). CCPN Route 2015. Recuperado el 4 Septiembre del 2015, de https://learningnetworkstore.cisco.com/on-demand-e-learning/cisco-for-ccnp-route-v2-0-180-day-subscription-elt-ccnpr-v2-0-020141

Salazar, L. (s.f.). Arquitectura de redes MPLS. Quito, Recuperado el 5 Septiembre del 2015, de https://learningnetworkstore.cisco.com/on-demand-e-learning/cisco-for-ccnp-route-v2-0-180-day-subscription-elt-ccnpr-v2-0-020141

Salazar, L. (s.f.). Implementación de Calidad de Servicio QoS. Recuperado el 6 Septiembre del 2015, de https://learningnetworkstore.cisco.com/on-demand-e-learning/cisco-for-ccnp-route-v2-0-180-day-subscription-elt-ccnpr-v2-0-020141

mahidol.ac (s.f). Implementación IPv6. Recuperado 8 de Septiembre de 2015, de

http://www.sc.mahidol.ac.th/scsosd/Doc/km/Network/CCNP/en_ROUTE_v6_Ch07 (IPv6).pdf

Redes-Linux.com. (s.f.). Sistema Autónomo y BGP. Recuperado el 9 de Septiembre de 2015, de http://www.redes-linux.com/manuales/routing/PIAM-Routing-BGP-v4.pdf

pcecuador.com. (s.f.). Observium en Centos. Recuperado el 9 de Septiembre de 2015, de http://www.pcecuador.com/web/index.php?option=com_content&view=article&id=235:ob&catid=150:laboratorios-linux-experto&Itemid=516

observium.org. (s.f.). Comuniadad del observium Recuperado el 10 de Septiembre de 2015, de http://www.observium.org/

James, R. (2013). EtherChannel. Recuperado el 9 de Septiembre de 2015, de http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/150_2_EX/layer2/configuration_guide/b_lay2_152ex_2960-x_cg.pdf

ANEXOS

ANEXOS 1

OSI. Modelo de interconexión de sistemas abiertos, indica las 7 capas por la que tiene que viajar los datos para comunicación entre dispositivos.
UTP. Par trenzado sin blindaje, empleado en las redes para las comunicaciones entre equipos como router, sitwich, etc.

MIMO. Múltiple entrada y múltiple salida, aumentando la eficiencia espectral y tasa de transferencia de las comunicaciones inalámbricas.
dB. Decibelio es una unidad adimensional, logarítmica y relativa, obtenida entre la relación de dos magnitudes la de estudio y de referencia.
HUB. Es una estación terrestre que retransmite la información de la estaciones satelitales.
QoS. Calidad de servicio, permite el transporte de tráfico con prioridad de cada servicio.
TTL. Tiempo de vida, es el tiempo que un paquete se encuentra por la red antes de ser descartado.
MTU. Unidad máxima de trasmisión, es el tamaño del paquete que se transmite en la red.
DSCP. Diferencia la calidad de los servicios que transportan a través de la red.
PVNs. Red privada virtual, es una comunicación entre dos redes de forma segura.
PBR. Policy Based Routing, políticas para cambiar el enrutamiento de determinadas redes mediante route-map.
LER. Router de border de etiquetas está en la salida o entrada de la red MPLS, que realiza la función de poner o quitar etiquetas.
VRF. Reenvió y enrutamiento virtual, crea diferentes tablas de enrutamiento en un mismo equipo físico.
NAT. Traslado de direcciones de red, cambio de una dirección privada o pública a otra dirección.

DHCP. Protocolo de configuración de host dinámico, asigna un dirección IP dinámicamente.

TCP. Protocolo de transmisión de información, garantiza para el transporte seguro entre equipos.

UDP. Protocolo de datagrama de usuarios, empleado para el transporte de datagramas.

ICMP. Protocolo de mensajes de control de internet.

IPsec. Protocolo de seguridad de internet, permite una comunicación extremo a extremo segura.

IGP. Protocolo de Gateway interior, son los protocolos que se encuentran en un mismo sistema autónomo.

ISP. Proveedor de servicio de internet.

GRE. Encapsulación de enrutamiento genérico, permite realizar PVN con túneles.

WAN. Red de área amplia, es una red conformado por varias partes físicas.

CNT. Corporación nacional de telecomunicaciones.

WIC2H. Tarjeta de red con 4 puertos RJ45 de capa 2.

SLA. Servicio de Valor Agregado.

ANEXOS 2

Configuración del router de matriz Quito en los que se encuentra los servicios de datos y acceso a internet para las sucursales.

URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#sh run
Building configuration...

Current configuration : 6012 bytes
!
! Last configuration change at 17:04:57 UTC Wed Nov 11 2015 by operador
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname URBANO_EXPRESS_DATOS_INTERNET_MATRIZ
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$6jlP$1m9Xkdm3dT68VURRCeKKc.
!
no aaa new-model
!
ip vrf datos
rd 2:2
route-target export 2:2
route-target import 2:2
!
ip vrf internet

```
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
license udi pid CISCO2921/K9 sn FGL1628139A
!
username uxxxxx privilege 15 password 7
1516185D11382925263C303A0315131012
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description DATOS_PRINCIPAL_CALIX
 ip vrf forwarding datos
 ip address 10.10.10.2 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description INTERNET_PRINCIPAL_CALIX
 ip vrf forwarding internet
```

```
 ip address 192.168.43.42 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description ENLACES_BK_DATOS_INTERNET_CORECESS
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2.3211
 description DATOS_BK_CORECESS
 encapsulation dot1Q 3211
 ip vrf forwarding datos
 ip address 10.10.10.6 255.255.255.252
!
interface GigabitEthernet0/2.3222
 description INTERNET_BK_CORECESS
 encapsulation dot1Q 3222
 ip vrf forwarding internet
 ip address 192.168.43.38 255.255.255.252
!
interface FastEthernet0/0/0
 switchport access vlan 20
 no ip address
!
interface FastEthernet0/0/1
 switchport access vlan 20
 no ip address
!
interface FastEthernet0/0/2
```

```
 description LAN_SALIDA_INTERNET
 switchport access vlan 11
 no ip address
!
interface FastEthernet0/0/3
 switchport access vlan 10
 no ip address
!
interface Vlan1
 no ip address
!
interface Vlan10
 description POOL_PUBLICAS_INTERNET
 ip vrf forwarding internet
 ip address 181.49.11.1 255.255.255.252
!
interface Vlan11
 description LAN_SALIDA_INTERNET
 ip vrf forwarding datos
 ip address 10.10.10.1 255.255.255.252
 shutdown
!
interface Vlan20
 description LAN_DATOS
 ip vrf forwarding datos
 ip address 192.168.1.7 255.255.255.0
!
router bgp 64514
 bgp router-id 10.10.10.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 !
```

address-family ipv4 vrf datos
network 192.168.1.0
redistribute static
neighbor 10.10.10.1 remote-as 56001
neighbor 10.10.10.1 description PRINCIPAL
neighbor 10.10.10.1 activate
neighbor 10.10.10.1 allowas-in
neighbor 10.10.10.1 route-map entrada_principal in
neighbor 10.10.10.1 route-map salida_principal_datos out
neighbor 10.10.10.5 remote-as 56001
neighbor 10.10.10.5 description BK_PE
neighbor 10.10.10.5 activate
neighbor 10.10.10.5 allowas-in
neighbor 10.10.10.5 route-map entrada_bk in
neighbor 10.10.10.5 route-map salida_BK_datos out
default-information originate
exit-address-family
!
address-family ipv4 vrf internet
network 181.49.11.0 mask 255.255.255.252
neighbor 192.168.43.37 remote-as 56001
neighbor 192.168.43.37 local-as 64700
neighbor 192.168.43.37 description PRINCIPAL
neighbor 192.168.43.37 activate
neighbor 192.168.43.37 route-map entrada_principal in
neighbor 192.168.43.37 route-map salida_principal_internet out
neighbor 192.168.43.41 remote-as 56001
neighbor 192.168.43.41 local-as 64700
neighbor 192.168.43.41 description BK
neighbor 192.168.43.41 activate
neighbor 192.168.43.41 route-map entrada_bk in
neighbor 192.168.43.41 route-map salida_BK_internet out

```
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route vrf datos 0.0.0.0 0.0.0.0 10.10.10.2
ip route vrf datos 10.0.0.0 255.255.255.252 192.168.1.82
ip route vrf datos 10.0.5.0 255.255.255.252 192.168.1.82
ip route vrf datos 10.0.6.0 255.255.255.252 192.168.1.82
ip route vrf datos 172.16.1.0 255.255.255.0 192.168.1.82
ip route vrf datos 192.168.2.0 255.255.255.0 192.168.1.82
ip route vrf datos 192.168.41.0 255.255.255.0 192.168.1.82
ip route vrf datos 192.168.42.0 255.255.255.0 192.168.1.82

!
!
route-map entrada_principal permit 10
 set local-preference 350
!
route-map entrada_principal deny 20
!
route-map salida_BK_datos permit 10
 set as-path prepend 64514 64514 64514
!
route-map salida_BK_datos deny 20
!
route-map salida_principal_internet permit 10
 set as-path prepend 64700
!
route-map salida_principal_internet deny 20
```

!
route-map salida_BK_internet permit 10
set as-path prepend 64700 64700 64700
!
route-map salida_BK_internet deny 20
!
route-map salida_principal_datos permit 10
!
route-map salida_principal_datos deny 20
!
route-map entrada_bk permit 10
set local-preference 200
!
route-map entrada_bk deny 20
!
!
snmp-server community xxxxx RO
!
control-plane
!
!
banner motd ^C

PUNTONET S.A.
Acceso restringido!!!

Solo personal autorizado - FC.

Fecha: 2015_08_07 E-mail: cccorporativo@puntonet.ec
Empresa: URBANO_EXPRESS_MATRIZ_DATOS_INTERNET

```
---------------------------------------------------------------------
^C
!
line con 0
 password 7 06161A2F58410D18111801
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 06021C70595C0B180B1817131C162F3837
 login local
 transport input all
!
scheduler allocate 20000 1000
!
End

URBANO_EXPRESS_DATOS_INTERNET_MATRIZ#
```